Introduzione e applicazioni di ARITMETICA MODULARE

Prof. Bruno Picasso

13 maggio 2019

Indice

1 Gli interi modulo n

1.1 Dalla retta numerica alla rappresentazione circolare dei numeri

Il modo comune per rappresentare i numeri è disporli sulla cosiddetta retta numerica. Poiché i punti di una retta possono essere *ordinati* (ossia, dati due punti A e B su una retta, si può dire se A *precede o segue* B), tale rappresentazione è adatta alle situazioni in cui il numero rappresenta grandezze per cui abbia senso parlare di quantità *maggiore o minore*. Ad esempio, il tempo e la temperatura sono grandezze le cui misure sono rappresentate da numeri sulla retta e la relazione "maggiore/minore" corrisponde, per il tempo, alla relazione "istante successivo/precedente", per la temperatura, a "più caldo/più freddo".
Vi sono però molte situazioni e fenomeni che si prestano ad essere descritti attraverso numerazioni che procedono in modo ciclico, anziché lineare, e che quindi presuppongono una rappresentazione dei numeri disposti non più su una retta bensì su una circonferenza.

Esempio 1 *Supponiamo di voler svolgere dei conti inerenti il susseguirsi delle stagioni, ad esempio: se oggi siamo in estate, in che stagione saremo tra 14 stagioni?*
Per rispondere a questa domanda possiamo numerare le stagioni in modo progressivo assegnando, ad esempio, all'inverno il numero 0, alla primavera l'1, all'estate il 2 e il 3 all'autunno. Poiché le stagioni si susseguono in modo ciclico, lo stesso dovrà accadere per la loro rappresentazione numerica: quindi il 4, dovendo rappresentare la stagione successiva alla numero 3, ossia l'inverno, sarà naturale posizionarlo laddove è posizionato lo 0. Allo stesso modo, è naturale far coincidere la posizione del 5 con quella dell'1, come pure far coincidere il 6 con il 2, il 7 con il 3 e così via. In tal modo, è come se la retta dei numeri venisse arrotolata con periodo 4 su una circonferenza (vedi Figura 1).

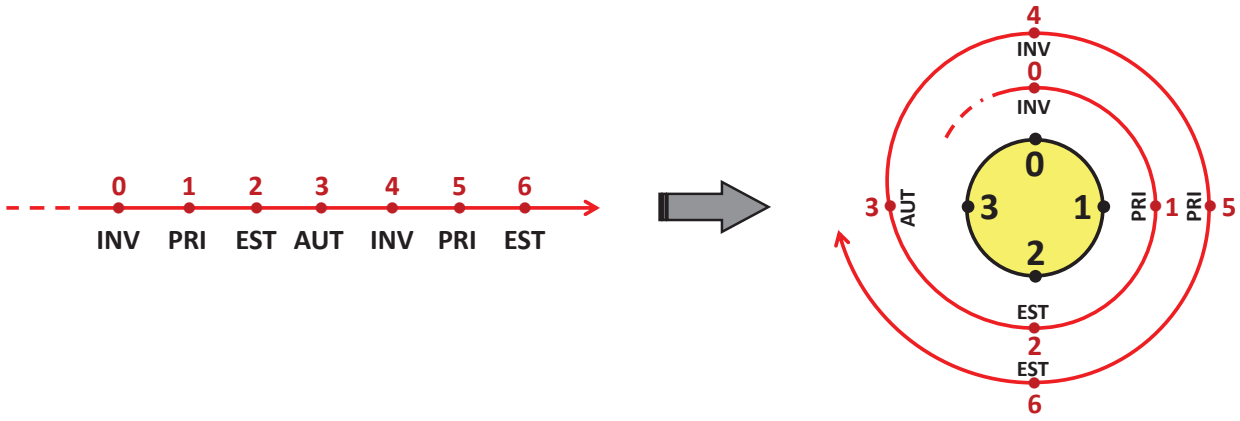


Figura 1: Dalla rappresentazione lineare dei numeri ad una circolare di periodo 4.

Usando tale rappresentazione, alla domanda iniziale si potrà quindi rispondere nel modo seguente: poiché all'estate corrisponde il numero 2, tra 14 stagioni saremo nella stagione numero $2+14=16$ e, nella rappresentazione circolare dei numeri, il 16 corrisponde allo 0, ossia saremo in inverno.

Diversamente da quanto accade per i punti di una retta, i punti di una circonferenza non possono essere ordinati, ossia non ha senso dire che un punto di una circonferenza precede o segue un altro punto. Le situazioni e i fenomeni che si prestano ad essere descritti attraverso numerazioni cicliche saranno quindi intrinsecamente caratterizzati da tale mancanza di ordinamento. Nell'esempio delle stagioni, ad esempio, non ha senso domandarsi se l'inverno preceda l'estate o viceversa (la risposta non è univoca, se ci poniamo la domanda il 10 Aprile saremo portati a rispondere che l'estate precede l'inverno ma se la stessa domanda ce la poniamo il 10 Ottobre daremo una risposta diversa).
Alcuni altri esempi di situazioni che sono descritte da numerazioni cicliche sono:

A. Il susseguirsi delle ore su un orologio: in tal caso la retta dei numeri viene "arrotolata" su una circonferenza con periodo 12. Ad esempio: se un orologio sta segnando le 7, tra 9 ore segnerà le 4 ($9+7=16$ e il 16 si posiziona laddove si trova il 4).

B. Il susseguirsi dei giorni della settimana (periodo 7).

C. La posizione di una ruota misurando gli angoli in gradi (periodo 360). Ad esempio, se ad una ruota viene imposta una rotazione di 180 gradi seguita da una rotazione di ulteriori 270 gradi, al termine essa avrà ruotato per complessivi 450 gradi e si troverà nella stessa posizione che occuperebbe se fosse stata ruotata di 90 gradi, vedi Figura 2.

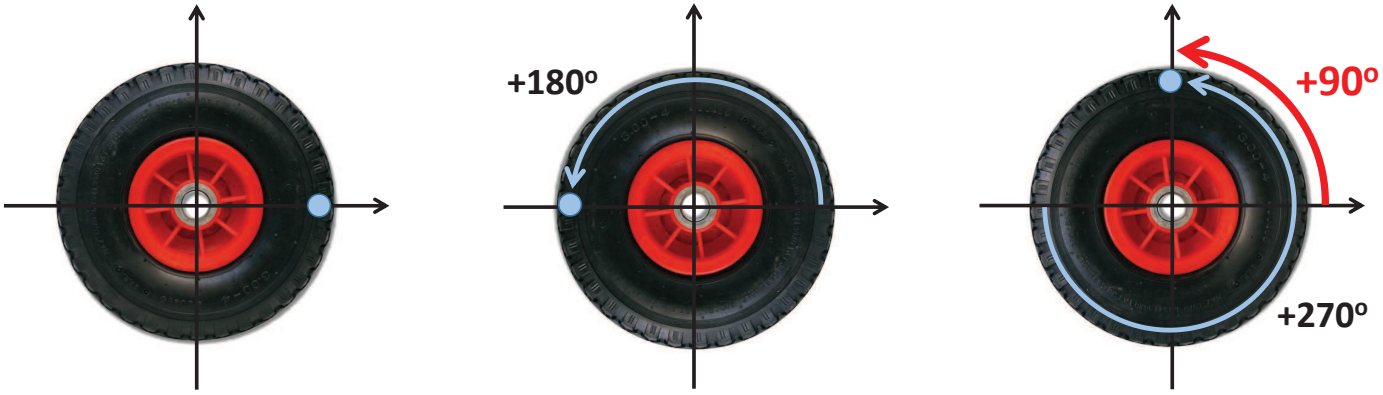


Figura 2: Una rotazione di $180+270$ gradi equivale ad una rotazione di 90 gradi rispetto alla posizione iniziale.

Quesito 1 *In modo analogo a quanto fatto per l'Esempio 1, mostra attraverso esempi che i tre casi A, B, C fanno riferimento a situazioni caratterizzate dalla mancaza di un ordinamento.*

Quesito 2 *Individua altri esempi di fenomeni/grandezze la cui rappresentazione naturale mediante numeri ha struttura ciclica: specifica il periodo e fornisci qualche esempio di calcolo inerente l'esempio considerato.*

Questioni riguardanti il susseguirsi delle stagioni (Esempio 1) avranno alla fine una risposta che potrà essere solo inverno, primavera, estate o autunno ossia, numericamente, solo 0, 1, 2 o 3. Tutti gli altri numeri sono ridondanti perché equivalenti ai quattro numeri di riferimento per le stagioni: il 4, l'8, il 12, etc. sono equivalenti allo 0 perché tutti corrispondono all'inverno; il 5, il 9, il 13, etc. sono equivalenti all'1 perché tutti corrispondono alla primavera, e così via. Allo stesso modo, qualunque calcolo riguradante il susseguirsi delle ore su un orologio potrà concludersi solo con un numero compreso tra 0 e 11 e, nel caso della posizione di una ruota, i numeri di riferimento sono quelli compresi tra 0 e 359.
In generale, nei problemi che presuppongono una rappresentazione dei numeri interi in modo circolare con periodo n, l'insieme numerico di riferimento è dato dai numeri compresi tra 0 e $n-1$: chiamiamo $\mathbb{Z}_n$ tale insieme. Dunque, dato un numero naturale $n \geq 2$, si ha

$$\mathbb{Z}_n = \{\, 0\,,\, 1\,,\, 2\,,\, \cdots\,,\, n-1 \,\}$$

In particolare:

$$\mathbb{Z}_2 = \{\, 0\,,\, 1 \,\} \qquad \mathbb{Z}_3 = \{\, 0\,,\, 1\,,\, 2 \,\} \qquad \mathbb{Z}_4 = \{\, 0\,,\, 1\,,\, 2\,,\, 3 \,\}$$
$$\mathbb{Z}_5 = \{\, 0\,,\, 1\,,\, 2\,,\, 3\,,\, 4 \,\} \qquad \mathbb{Z}_6 = \{\, 0\,,\, 1\,,\, 2\,,\, 3\,,\, 4\,,\, 5 \,\} \qquad \text{etc.}$$

Quando, come nell'Esempio 1, i numeri interi sono rappresentati in forma circolare con periodo 4, si parla di "numeri interi *modulo* 4". In generale, si parla di "**numeri interi *modulo* n**". Nella parte sinistra della Figura 3 sono rappresentati i numeri interi modulo 4 (la spirale rossa), in giallo l'insieme $\mathbb{Z}_4$ e tutti i numeri all'interno di uno dei quattro spicchi (ad esempio, -3, 1, 5, etc.) sono equivalenti. A destra sono invece rappresentati i numeri interi modulo 6, la porzione in giallo rappresenta l'insieme $\mathbb{Z}_6$ e tutti i numeri all'interno di uno dei sei spicchi (ad esempio, -5, 1, 7, 13, etc.) sono equivalenti. Naturalmente, al variare di n si crea una diversa rappresentazione dei numeri interi con differenti insiemi di numeri tra loro equivalenti.

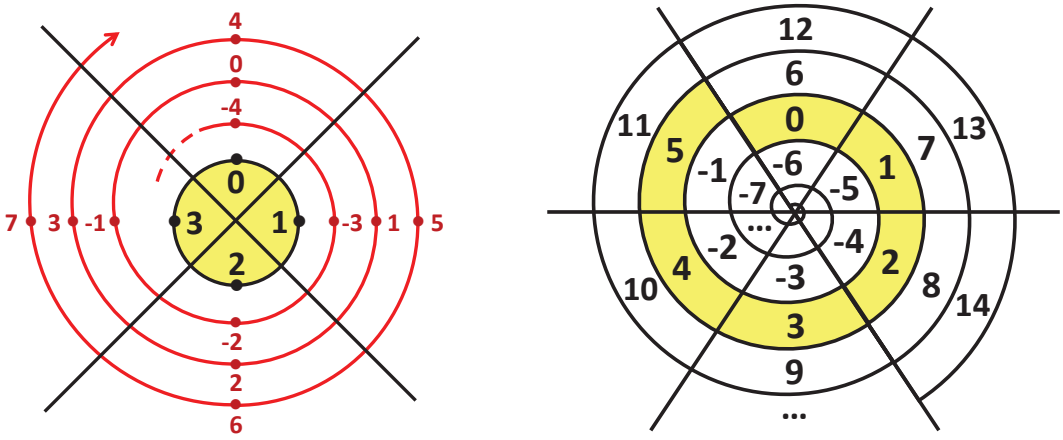


Figura 3: Rappresentazioni grafiche degli interi modulo n: a sinistra, gli interi modulo 4; a destra, gli interi modulo 6.

1.2 Punto di vista algebrico: da $\mathbb{Z}$ a $\mathbb{Z}_n$

Gran parte di quanto discusso nel paragrafo precedente può essere sintetizzato dicendo che, quando consideriamo i numeri interi modulo n, ogni numero intero risulta equivalente ad infiniti altri numeri interi e tra questi ce ne è uno speciale che è l'unico compreso tra 0 e $n-1$, ossia che sta nell'insieme $\mathbb{Z}_n$. Abbiamo quindi bisogno di strumenti algebrici che permettano di rispondere ai seguenti due quesiti fondamentali:

Q1. Dato un numero intero, a quale numero dell'insieme di riferimento $\mathbb{Z}_n$ è equivalente?

Q2. Dati due numeri interi, come si fa a determinare se sono equivalenti?

È sufficiente ripensare agli esempi numerici visti nel paragrafo precedente, in particolare la Figura 3 che si riferisce ai casi $\mathbb{Z}_4$ e $\mathbb{Z}_6$, per rendersi conto che:

R1. Dato un qualsiasi numero intero $z \in \mathbb{Z}$, il suo corrispettivo in $\mathbb{Z}_n$ è **il resto della divisione di z per n**.
Alla ricerca di tale corrispettivo ci si riferisce come alla "***riduzione* di z modulo n**".

R2. Dati due numeri interi $z_1 \in \mathbb{Z}$ e $z_2 \in \mathbb{Z}$ essi sono equivalenti se e solo se differiscono per un multiplo del periodo, ossia se $z_2 - z_1$ **è divisibile per n**.
La notazione che si usa per indicare che due numeri z_1 e z_2 sono equivalenti negli interi modulo n è

$$z_1 = z_2 \pmod{n}$$

e in tal caso si dice che "z_1 **è equivalente a z_2 modulo n**".

Esempio 2

1. *Consideriamo gli interi modulo 4, si ha:*
   - *Il corrispettivo di 11 in $\mathbb{Z}_4$ è 3, ossia $11 = 3 \pmod 4$, perché 11 diviso 4 fa 2 con il resto di 3 (vedi R1), o anche perché $11 - 3 = 8$ è divisibile per 4 (vedi R2).*
   - *Il numero 20 è equivalente a 0 negli interi modulo 4, ossia $20 = 0 \pmod 4$, perché 20 è divisibile per 4 (e quindi la divisione di 20 per 4 ha resto nullo).*
   - $23 = 59 \pmod 4$ *perché $59 - 23 = 36$ è divisibile per 4 e la loro riduzione modulo 4 è 3: $59 = 23 \pmod 4 = 3 \pmod 4$.*
   - $-13 \neq 22 \pmod 4$ *perché $22 - (-13) = 22 + 13 = 35$ non è divisibile per 4.*
2. *Consideriamo gli interi modulo 6, si ha:*
   - *La riduzione di 11 modulo 6 è 5, ossia $11 = 5 \pmod 6$, perché 11 diviso 6 fa 1 con il resto di 5 (vedi Figura 3).*
   - *I numeri equivalenti a 2 modulo 6 sono: 8, 14, 20, ... nonché -4, -10, -16 e così via. Per ottenerli basta aggiungere o togliere a 2 un multiplo di 6. L'insieme di tutti i numeri equivalenti a 2 si può quindi scrivere come $2 + 6k$, $k \in \mathbb{Z}$.*

Esempio 3 (La riduzione modulo n di numeri negativi) *Talvolta per i numeri negativi risulta meno immediato individuare il corrispettivo in $\mathbb{Z}_n$. Indicato con $-m$ un numero intero negativo, un modo facile di procedere per individuare la sua riduzione modulo n è il seguente:*

(1) si cambia di segno al numero dato e si ottiene $m > 0$;

(2) si individua il corrispettivo di m in $\mathbb{Z}_n$ e si ottiene un numero h;

(3) si cambia di segno ad h e si ottiene un numero $-h$ tale che $-n < -h < 0$;

(4) si aggiunge n al risultato e si ottiene $-h + n \in \mathbb{Z}_n$.

In questa procedura, l'unico numero di cui si calcola il corrispettivo in $\mathbb{Z}_n$ è m che è positivo.

- *È facile vedere che $-7 = 1 \pmod 4$ (basta aggiungere 8, che è multiplo di 4, al -7). Oppure, seguendo la procedura descritta sopra, si ha:*

$$-7 \xrightarrow{(1)} 7 \xrightarrow{(2)} 3 \xrightarrow{(3)} -3 \xrightarrow{(4)} -3 + 4 = 1$$

- *Calcoliamo il corrispettivo di -45 in $\mathbb{Z}_7$:*

$$-45 \xrightarrow{(1)} 45 \xrightarrow{(2)} 3\,(45 \text{ diviso } 7 \text{ fa } 6 \text{ con il resto di } 3) \xrightarrow{(3)} -3 \xrightarrow{(4)} -3 + 7 = 4\,,$$

quindi $-45 = 4 \pmod 7$.

La procedura funziona perché: $h = m \pmod n$ (passaggio 2) e quindi $-h = -m \pmod n$ (passaggio 3) ma anche $-h + n = -m \pmod n$ (passaggio 4) perché, aggiungendo a $-h$ un multiplo di n, si ottiene un elemento equivalente.

Osservazione 1 *Quando negli interi modulo 4 affermiamo che, ad esempio, il 3 e il 7 sono* equivalenti*, intendiamo dire che, pur essendo due numeri diversi, essi rappresentano la stessa cosa e quindi sono intercambiabili: nell'esempio delle stagioni il 3 e il 7 sono solo due modi diversi di individuare l'autunno. Per quanto possa sembrare strano considerare uguali il 3 e il 7, questa situazione è analoga a quel che accade nell'insieme delle frazioni. Ad esempio, siamo già abituati al fatto che, sebbene $\frac{1}{2}$ e $\frac{2}{4}$ siano due frazioni differenti, esse siano totalmente intercambiabili perché rappresentano lo stesso numero. Nel contesto delle frazioni affermiamo appunto che $\frac{1}{2}$ e $\frac{2}{4}$ sono* equivalenti*. In questo parallelismo tra numeri interi modulo n e frazioni, il problema della riduzione modulo n di un dato numero intero è quindi analogo a quello della riduzione ai minimi termini di una frazione.*

2 Aritmetica in $\mathbb{Z}_n$

Abbiamo introdotto i numeri interi modulo n come un modello matematico alternativo a quello della retta numerica evidenziando l'esistenza di situazioni che si prestano meglio ad essere

descritte attraverso una rappresentazione circolare dei numeri. Questo nuovo modello sarebbe di poca utilità pratica se con esso non fosse possibile svolgere calcoli o risolvere equazioni. In questo paragrafo ci occupiamo quindi di introdurre dapprima le operazioni di somma e prodotto tra gli elementi di $\mathbb{Z}_n$, quindi mostreremo come dalle proprietà di queste operazioni si possano far discendere metodi efficaci per la risoluzione del problema della riduzione modulo n di un numero intero. Affronteremo poi il problema dell'operazione inversa al prodotto (la divisione) che, come in $\mathbb{Z}$, non sempre è possibile; saremo così in grado di risolvere semplici equazioni di primo grado in $\mathbb{Z}_n$. Presenteremo infine, senza dimostrarla, un'identità fondamentale dell'aritmetica modulare, il cosiddetto "Teorema di Eulero-Fermat", che sarà alla base del funzionamento di un algoritmo di crittografia che introdurremo nel paragrafo successivo.

2.1 La somma (algebrica) in $\mathbb{Z}_n$

Quando si considera l'insieme $\mathbb{Z}$ dei numeri interi, sommare corrisponde sulla retta numerica a procedere nel verso concorde all'orientamento della retta (tipicamente verso destra) della quantità che si sta sommando, sottrarre (ossia, sommare un numero negativo) corrisponde a procedere nel verso opposto (tipicamente verso sinistra); il risultato di una somma algebrica tra numeri interi è ancora un numero intero, si dice cioè che la somma è un'operazione *interna*. Nel caso di $\mathbb{Z}_n$, la procedura va adattata al fatto che $\mathbb{Z}_n$ ha una struttura circolare (Figura 4.A): sommare corrisponde a procedere in senso orario (Figura 4.B), sottrarre a procedere in senso antiorario (Figura 4.C); affinché l'operazione sia *interna*, e dunque il risultato sia ancora un elemento di $\mathbb{Z}_n$, bisogna inoltre rispettare il fatto che, nel procedere in senso orario (sommando), dopo $n-1$ si presenta nuovamente lo 0, poi l'1 e così via, nel procedere in senso antiorario (sottraendo), la sequenza da seguire è 1, 0, $n-1$, $n-2$, etc.

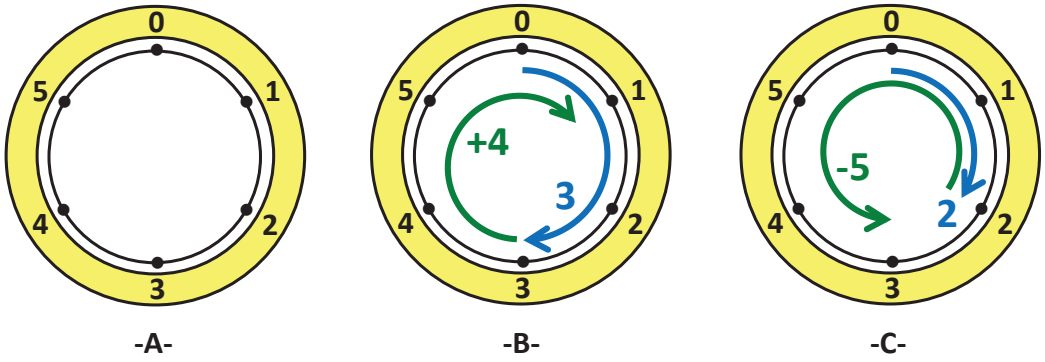


Figura 4: **-A-** L'insieme $\mathbb{Z}_6$ **-B-** La somma in $\mathbb{Z}_6$ **-C-** Sottrazione in $\mathbb{Z}_6$.

Ad esempio, in $\mathbb{Z}_6$, avremo (vedi Figura 4):

$$2+3=5 \ (\text{mod } 6) \qquad 3+4=1 \ (\text{mod } 6) \qquad 4+2=0 \ (\text{mod } 6)$$
$$4-2=2 \ (\text{mod } 6) \qquad 2-5=3 \ (\text{mod } 6) \qquad -2-3=1 \ (\text{mod } 6)$$

Somma e sottrazioni si eseguono in modo analogo a come si eseguono su un orologio: per $\mathbb{Z}_n$ si tratta di un "orologio" da n ore, l'orologio standard fornisce il modello per l'insieme $\mathbb{Z}_{12}$. Come risulta chiaro anche dal confronto tra le Figure 4 e 3, nella pratica:

> Somme e sottrazioni tra elementi di $\mathbb{Z}_n$ si possono eseguire svolgendo il calcolo in $\mathbb{Z}$ e riducendo il risultato modulo n.

Ad esempio:

$$3+4=7\ (\text{mod}\ 6)=1\ (\text{mod}\ 6) \qquad \text{oppure} \qquad 2-5=-3\ (\text{mod}\ 6)=3\ (\text{mod}\ 6)\,,$$

o anche, riprendendo quanto fatto nell'Esempio 1 sulle stagioni,

$$2+14=16\ (\text{mod}\ 4)=0\ (\text{mod}\ 4)$$

Questo modo di procedere è del tutto coerente con il fatto che numeri interi diversi ma equivalenti $\big($il 7 e l'1 nel caso di $3+4=1\ (\text{mod}\ 6)$, oppure il 16 e lo 0 nel caso di $2+14=0\ (\text{mod}\ 4)\big)$ individuano lo stesso elemento di $\mathbb{Z}_n$ (nell'esempio delle stagioni, 0 e 16 individuano comunque l'inverno). Inoltre, la riduzione modulo n del passaggio finale assicura che la somma algebrica sia un'operazione *interna* a $\mathbb{Z}_n$. Riassumendo[1]:

> Quando si svolge un qualsiasi calcolo in $\mathbb{Z}_n$, ci si può avvalere dell'ausilio dell'insieme $\mathbb{Z}$ ma, al termine delle operazioni, si deve ridurre modulo n il numero ottenuto. Il risultato finale del calcolo deve essere un elemento di $\mathbb{Z}_n$, ossia un numero compreso tra 0 e $n-1$.

Osservazione 2 *Come appena visto e come discusso nell'Osservazione 1, negli interi modulo n i numeri equivalenti sono intercambiabili: ciò significa che, al bisogno, anche* **nell'eseguire le operazioni è possibile sostituire un numero con uno ad esso equivalente***. Ad esempio:*

$$4=-2\ (\textit{mod}\ 6) \quad \textit{quindi} \quad 3+4=3-2\ (\textit{mod}\ 6)=1\ (\textit{mod}\ 6) \quad \textit{oppure}$$
$$-5=1\ (\textit{mod}\ 6) \quad \textit{quindi} \quad 2-5=2+1\ (\textit{mod}\ 6)=3\ (\textit{mod}\ 6)$$

2.2 Il prodotto in $\mathbb{Z}_n$

Per la moltiplicazione si procede in modo del tutto analogo a quanto visto per la somma algebrica, ossia:

> I prodotti tra elementi di $\mathbb{Z}_n$ si possono eseguire svolgendo il calcolo in $\mathbb{Z}$ e riducendo il risultato modulo n.

[1] Riferendosi al parallelismo tra frazioni e numeri interi modulo n introdotto nell'Osservazione 1, sommare in $\mathbb{Z}$ e ridurre modulo n è la procedura analoga a sommare le frazioni e poi ridurre ai minimi termini: ad esempio, $\frac{3}{4}+\frac{7}{4}=\frac{10}{4}=\frac{5}{2}$ oppure $\frac{3}{10}+\frac{1}{14}=\frac{26}{70}=\frac{13}{35}$.

Ad esempio:

$$\begin{array}{lll} 3\cdot 5 = 3 \ (\text{mod } 6) & \text{perché} & 3\cdot 5 = 15 \ (\text{mod } 6) = 3 \ (\text{mod } 6) \\ 3\cdot 5 = 1 \ (\text{mod } 7) & \text{perché} & 3\cdot 5 = 15 \ (\text{mod } 7) = 1 \ (\text{mod } 7) \\ 2\cdot 6 = 0 \ (\text{mod } 12) & \text{perché} & 2\cdot 6 = 12 \ (\text{mod } 12) = 0 \ (\text{mod } 12) \end{array}$$

L'ultimo esempio mette in evidenza una particolarità dell'insieme $\mathbb{Z}_n$ che lo distingue da tutti gli insiemi numerici precedentemente conosciuti, ossia il fatto che, in generale, in $\mathbb{Z}_n$ **non vale la legge di annullamento del prodotto**, ossia, in $\mathbb{Z}_n$ non è vero che se il prodotto tra due numeri è 0 allora almeno uno dei due fattori deve essere nullo. Torneremo su questo punto in maggior dettaglio nel Paragrafo 2.4.
L'esempio seguente mostra che, nello svolgere i prodotti, risulta particolarmente utile giovarsi della possibilità di sostituire un numero con un altro equivalente (vedi l'Osservazione 2).

Esempio 4

1. *In* $\mathbb{Z}_{12}$, $3\cdot 5\cdot 7 = 9 \ (\textit{mod } 12)$, *infatti:*
   - $3\cdot 5\cdot 7 = 105 \ (\textit{mod } 12) = 9 \ (\textit{mod } 12)$ *(perché* 105 *diviso* 12 *fa* 8 *con il resto di* 9*);*
   - *oppure, più semplicemente,* $3\cdot 5\cdot 7 = 15\cdot 7 \ (\textit{mod } 12) \overset{(a)}{=} 3\cdot 7 \ (\textit{mod } 12) = 21 \ (\textit{mod } 12) = 9 \ (\textit{mod } 12)$ *(dove, nell'uguaglianza (a), abbiamo sostituito* 15 *con* 3 *perché* $15 = 3 \ (\textit{mod } 12)$*);*
   - *o anche,* $3\cdot 5\cdot 7 = 3\cdot 35 \ (\textit{mod } 12) \overset{(b)}{=} 3\cdot(-1) \ (\textit{mod } 12) = -3 \ (\textit{mod } 12) = 9 \ (\textit{mod } 12)$ *(dove, nell'uguaglianza (b), abbiamo sostituito* 35 *con* -1 *perché* $35 = -1 \ (\textit{mod } 12)$*).*
2. *In* $\mathbb{Z}_{60}$, $58^6 = 4 \ (\textit{mod } 60)$, *infatti:* $58^6 = (-2)^6 \ (\textit{mod } 60) = 64 \ (\textit{mod } 60) = 4 \ (\textit{mod } 60)$.

2.3 Strategie per la riduzione modulo n e criteri di divisibilità

In questo paragrafo ci soffermeremo su alcune strategie di calcolo in $\mathbb{Z}_n$ e, principalmente, sulla riduzione modulo n di un numero. Mostreremo con particolare rilievo come la possibilità di sostituire in un'espressione un numero con uno ad esso equivalente permetta in molti casi di semplificare i calcoli. Ci limiteremo a considerare numeri positivi perché, come visto nell'Esempio 3, la riduzione di numeri negativi può sempre essere calcolata mediante una procedura che prevede solo la riduzione di numeri positivi.
Osserviamo inoltre che saper risolvere il problema della riduzione modulo n dà immediata soluzione al problema di stabilire se un dato numero sia divisibile per n, infatti:

Dire che un numero m è divisibile per n è la stessa cosa che dire che $m = 0 \ (\text{mod } n)$.

Dunque, per stabilire se m è divisibile per n è sufficiente ridurlo modulo n e vedere se il risultato è 0 oppure no.

Tratteremo nel dettaglio tutti i casi in cui n è compreso tra 2 e 11. Prima però illustriamo le principali procedure attraverso un esempio: sebbene l'esempio farà sostanzialmente riferimento al caso specifico di $\mathbb{Z}_6$, da esso trarremo alcuni principi generali che possono essere efficacemente applicati per qualsiasi altro valore di n.

Esempio 5 (Metodi primari di riduzione modulo n) *Ridurre modulo 6 il numero $m = 729$. Tutte le tecniche che presenteremo si basano sulla riscrittura in forma polinomiale (anziché posizionale) del numero da ridurre, nel nostro caso:*

$$729 = \underbrace{7 \cdot 10^2 + 2 \cdot 10 + 9}_{\text{Forma polinomiale}} \tag{1}$$

• **Metodo base (riduzione delle potenze di 10):** *calcoliamo la riduzione modulo 6 di 10 e di 10^2 e sostituiamo il loro equivalente in $\mathbb{Z}_6$ nell'espressione polinomiale di m. Si ha:*

$$\begin{cases} 10 = & 4 \ (\textit{mod}\ 6) \\ 10^2 = & 10 \cdot 10 \ (\textit{mod}\ 6) \overset{(a)}{=} 4 \cdot 4 \ (\textit{mod}\ 6) = 16 \ (\textit{mod}\ 6) = 4 \ (\textit{mod}\ 6), \end{cases}$$

dove nell'uguaglianza (a) abbiamo sostituito 10 con 4 in quanto, come visto alla riga sopra, 10 e 4 sono equivalenti modulo 6. Quindi,

$$\begin{aligned} m = 729 = & \ 7 \cdot 10^2 + 2 \cdot 10 + 9 \ (\textit{mod}\ 6) \overset{(b)}{=} 7 \cdot 4 + 2 \cdot 4 + 9 \ (\textit{mod}\ 6) = \\ = & \ 28 + 8 + 9 \ (\textit{mod}\ 6) = 45 \ (\textit{mod}\ 6) = 3 \ (\textit{mod}\ 6), \end{aligned}$$

dove, per l'appunto, nell'uguaglianza (b) abbiamo sostituito sia 10 che 10^2 con 4 in virtù delle equivalenze vista sopra.

Osservazione 3 *Nota che, giunti all'espressione $28+8+9 \ (\textit{mod}\ 6)$, il calcolo della riduzione può essere completato in diversi altri modi, ad esempio:*

$$m = 729 = (28 + 8) + 9 \ (\textit{mod}\ 6) \overset{(c)}{=} 0 + 3 \ (\textit{mod}\ 6),$$

dove nell'uguaglianza (c) si usa il fatto che $28 + 8 = 36$ è equivalente a 0 e 9 è equivalente a 3 modulo 6. Oppure si può iterare la riduzione delle potenze di 10:

$$m = 729 = 45 \ (\textit{mod}\ 6) = 4 \cdot 10 + 5 \ (\textit{mod}\ 6) = 4 \cdot 4 + 5 \ (\textit{mod}\ 6) = 21 \ (\textit{mod}\ 6) = 3 \ (\textit{mod}\ 6).$$

E anche, a partire dall'espressione $4 \cdot 4 + 5 \ (\textit{mod}\ 6)$, si può concludere utilizzando l'equivalenza tra 5 e -1 in $\mathbb{Z}_6$:

$$m = 729 = 4 \cdot 4 + 5 \ (\textit{mod}\ 6) = 16 - 1 \ (\textit{mod}\ 6) = 15 \ (\textit{mod}\ 6) = 3 \ (\textit{mod}\ 6).$$

• **Metodo delle cifre (riduzione delle cifre):** *a partire dalla scrittura polinomiale del numero, invece di ridurre le potenze di 10, si possono ridurre i fattori corrispondenti alle cifre di m.*

Ossia:

$$\begin{aligned} m = \;& 729 = 7 \cdot 10^2 + 2 \cdot 10 + 9 \;(\textit{mod}\; 6) \overset{(\mathrm{d})}{=} 1 \cdot 10^2 + 2 \cdot 10 + 3 \;(\textit{mod}\; 6) = \\ = \;& 123 \;(\textit{mod}\; 6) = 3 \;(\textit{mod}\; 6)\,, \end{aligned}$$

dove nell'uguaglianza (d) abbiamo sostituito 7 *con* 1 *e* 9 *con* 3 *perché* $7 = 1 \;(\textit{mod}\; 6)$ *e* $9 = 3 \;(\textit{mod}\; 6)$*; inoltre* $123 = 3 \;(\textit{mod}\; 6)$ *perché* 120 *è divisibile per* 6*.*
Questo esempio ha messo in luce il seguente aspetto particolare dell'aritmetica in $\mathbb{Z}_n$*:*

> *Dato un numero* m*, se si sostituisce una sua cifra (o più) con una cifra equivalente modulo* n*, si ottiene un numero equivalente al numero dato.*

Infatti, sostituire una cifra di m *corrisponde a sostituire un fattore della corrispettiva scrittura polinomiale. Ad esempio, consideriamo il numero* $m = 98$*, si ha:*

$$\begin{aligned} 98 &= 10 \;(\textit{mod}\; 8) = 2 \;(\textit{mod}\; 8) \\ 98 &= 21 \;(\textit{mod}\; 7) = 0 \;(\textit{mod}\; 7) \\ 98 &= 32 \;(\textit{mod}\; 6) = 2 \;(\textit{mod}\; 6) \\ 98 &= 43 \;(\textit{mod}\; 5) = 3 \;(\textit{mod}\; 5) \\ 98 &= 02 \;(\textit{mod}\; 3) = 2 \;(\textit{mod}\; 3) \end{aligned}$$

Inoltre, come mostriamo nell'osservazione seguente, questo principio può essere impiegato non solo sulle cifre singole ma anche su gruppi di cifre.

Osservazione 4 (Sostituzione di gruppi di cifre) *Per ridurre l'espressione* $123 \;(\textit{mod}\; 6)$ *possiamo anche osservare che, non solo la scrittura* 123 *si interpreta come "*1 *centinaio,* 2 *decine e* 3 *unità", ossia* $123 = 1 \cdot 10^2 + 2 \cdot 10 + 3$*, ma anche come "*$12$ *decine e* 3 *unità", cioè* $123 = 12 \cdot 10 + 3$*. Quindi:*

$$m = 729 = 123 \;(\textit{mod}\; 6) = 12 \cdot 10 + 3 \;(\textit{mod}\; 6) = 0 \cdot 10 + 3 \;(\textit{mod}\; 6) = 3 \;(\textit{mod}\; 6)\,,$$

ossia il gruppo di cifre 12 *può essere sostituito con* 0 *perché* $12 = 0 \;(\textit{mod}\; 6)$*. Se ci si accorge che* 72 *è divisibile per* 6*, la stessa operazione poteva essere direttamente effettuata sul numero* 729 *e, in un unico passaggio, scrivere che*

$$m = 729 = 72 \cdot 10 + 9 \;(\textit{mod}\; 6) = 0 \cdot 10 + 3 \;(\textit{mod}\; 6) = 3 \;(\textit{mod}\; 6)\,.$$

Naturalmente, nel fare la sostituzione delle cifre, è importante mantenere la posizione di esse in quanto posizioni diverse corrispondono a differenti potenze di 10 *per cui si sta moltiplicando la cifra o il gruppo di cifre (e, in generale, potenze diverse di* 10 *hanno un diverso corrispettivo in* $\mathbb{Z}_n$*). Ad esempio, in* $\mathbb{Z}_7$*,*

$$9308 \overset{(\mathrm{e1})}{=} 2021 \;(\textit{mod}\; 7) \overset{(\mathrm{e2})}{=} 600 \;(\textit{mod}\; 7) \overset{(\mathrm{e3})}{=} 40 \;(\textit{mod}\; 7) = 5 \;(\textit{mod}\; 7)\,,$$

dove: nell'uguaglianza (e1) abbiamo sostituito la cifra 9 *con* 2*, il gruppo di cifre* 30 *con* 02 *(*$30 = 2 \ (\text{mod } 7)$*) e la cifra* 8 *con* 1*; nell'uguaglianza (e2) abbiamo sostituito il gruppo di cifre* 20 *con* 06 *(*$20 = 6 \ (\text{mod } 7)$ *e, ovviamente, non c'è bisogno di scrivere lo* 0 *iniziale) e il gruppo di cifre* 21 *con* 00 *(*21 *è divisibile per* 7*); infine, nell'uguaglianza (e3) abbiamo sostituito il gruppo di cifre* 60 *con* 4 *(*$60 = 4 \ (\text{mod } 7)$*).*
Oppure, in $\mathbb{Z}_{11}$*:*

$$59437 \overset{\text{(f1)}}{=} 50604 \ (\text{mod } 11) \overset{\text{(f2)}}{=} 6604 \ (\text{mod } 11) \overset{\text{(f3)}}{=} 4 \ (\text{mod } 11) \, ,$$

dove: nell'uguaglianza (f1) abbiamo sostituito il gruppo di cifre 94 *con* 06 *(*$94 = 6 \ (\text{mod } 11)$*) e il gruppo di cifre* 37 *con* 04 *(*$37 = 4 \ (\text{mod } 11)$*); nell'uguaglianza (f2) abbiamo sostituito il gruppo di cifre* 50 *con* 6 *(*$50 = 6 \ (\text{mod } 11)$*) e nell'uguaglianza (f3) abbiamo sostituito il gruppo di cifre* 66 *con* 0 *(*66 *è divisibile per* 11*).*

- **Metodo combinato :** *naturalmente il modo più efficace per semplificare i calcoli della riduzione è combinare i due metodi e ridurre sia le cifre che le potenze di* 10*. Si può procedere in modo simultaneo:*

$$m = 729 = 7 \cdot 10^2 + 2 \cdot 10 + 9 \ (\text{mod } 6) = 1 \cdot 4 + 2 \cdot 4 + 3 \ (\text{mod } 6) = 15 \ (\text{mod } 6) = 3 \ (\text{mod } 6) \, .$$

Oppure, nei casi più complessi, si possono alternare le due strategie: ad esempio, si può iniziare con qualche passaggio di riduzione delle cifre, anche a gruppi, in modo da rendere più piccoli i numeri da maneggiare, seguito dalla riduzione delle potenze del 10 *e, eventualmente, ripetere operazioni di riduzione delle cifre sul risultato ottenuto.*

In conclusione, prima di passare a considerare in dettaglio i vari moduli, è utile ribadire quanto già osservato diffusamente, e cioè che, in un'espressione, **vi è piena libertà di sostituire qualsiasi numero con uno ad esso equivalente** e i molteplici modi attraverso cui ci si può giovare di questa possibilità permettono di semplificare drammaticamente i calcoli in $\mathbb{Z}_n$.

2.3.1 Riduzione modulo 2

L'insieme $\mathbb{Z}_2 = \{ 0 , 1 \}$ è di gran lunga il più facile da trattare: i numeri pari sono equivalenti a 0, i numeri dispari sono equivalenti a 1.

2.3.2 Riduzione modulo 3 e modulo 9

Riduzione modulo 3
Al fine di utilizzare il metodo base, cominciamo con il calcolo della riduzione modulo 3 di 10

e delle sue potenze:

$$\begin{cases} 10 = 1 \ (\text{mod } 3) \\ 10^2 \overset{(a)}{=} 1^2 \ (\text{mod } 3) = 1 \ (\text{mod } 3) \\ \forall\, h \in \mathbb{N}\,,\ 10^h = 1^h \ (\text{mod } 3) = 1 \ (\text{mod } 3)\,, \end{cases}$$

dove nell'uguaglianza (a) abbiamo sostituito 10 con 1 perché, come visto sopra, 10 e 1 sono equivalenti in $\mathbb{Z}_3$. Dunque, **tutte le potenze di 10 sono equivalenti a 1 modulo 3.** Conseguentemente, come illustrato nell'esempio seguente, il solo uso del metodo base permette di risolvere facilmente il problema della riduzione modulo 3:

$$\begin{aligned} m = 412 = \ & 4 \cdot 10^2 + 1 \cdot 10 + 2 \ (\text{mod } 3) \overset{(b)}{=} 4 \cdot 1 + 1 \cdot 1 + 2 \ (\text{mod } 3) = \\ = \ & 4 + 1 + 2 \ (\text{mod } 3) = 7 \ (\text{mod } 3) = 1 \ (\text{mod } 3)\,, \end{aligned}$$

dove nell'uguaglianza (b) abbiamo sostituito le potenze di 10 con 1 in virtù dell'equivalenza vista sopra. Possiamo cioè affermare che

Ogni numero positivo è equivalente modulo 3 alla somma delle sue cifre.

Per ridurre modulo 3 un numero basta quindi sommare le sue cifre, ed eventualmente iterare la procedura sommando le cifre del risultato, finché si giunge ad un numero piccolo per cui è facile calcolare la riduzione.
Da quanto visto segue anche il ben noto criterio di divisibilità per 3, ossia: ***"un numero è divisibile per 3 se e solo se lo è la somma delle sue cifre"***.
Per quanto riguarda il metodo delle cifre, in $\mathbb{Z}_3$ vale la seguente proprietà: poiché tutte le potenze di 10 sono tra loro equivalenti modulo 3, la posizione delle cifre di un numero è ininfluente ai fini della riduzione. Dunque,

In $\mathbb{Z}_3$, cambiando l'ordine delle cifre di un numero (o anche eliminando le cifre nulle oppure cifre / gruppi di cifre multipli di 3), si ottiene un numero equivalente a quello iniziale.

Esempio 6 *Stabilire se il numero $m = 427831$ è divisibile per 3 e, se non lo è, trovare il numero divisibile per 3 più vicino a m.*
A tal fine, cominciamo con il ridurre 427831 modulo 3:

$$m = 427831 = 4 + 2 + 7 + 8 + 3 + 1 \ (\textit{mod } 3) = 25 \ (\textit{mod } 3) = 2 + 5 \ (\textit{mod } 3) = 1 \ (\textit{mod } 3)\,.$$

Dunque m non è divisibile per 3 e, essendo il resto della divisione di m per 3 pari a 1, il numero divisibile per 3 più vicino a m è il precedente di m, dunque 427830.
Naturalmente la riduzione di 427831 modulo 3 può essere calcolata in molti altri modi:

$$m = 427831 = (4 + 2) + (7 + 8) + 3 + 1 \ (\textit{mod } 3) \overset{(c)}{=} 0 + 0 + 0 + 1 \ (\textit{mod } 3) = 1 \ (\textit{mod } 3)\,,$$

dove nell'uguaglianza (c) si usa il fatto che 6, 15 *e* 3 *sono equivalenti a* 0 *modulo* 3. *Oppure, combinando con il metodo delle cifre,*

$$m = 427831 \overset{(d)}{=} 121201 \ (\textit{mod}\ 3) = 7 \ (\textit{mod}\ 3) = 1 \ (\textit{mod}\ 3)\,,$$

dove nell'uguaglianza (d) abbiamo ridotto modulo 3 *le singole cifre.*

Riduzione modulo 9

Poiché $10 = 1 \ (\text{mod}\ 9)$, anche **in** $\mathbb{Z}_9$ **tutte le potenze di** 10 **sono equivalenti a** 1, dunque:

Ogni numero positivo è equivalente modulo 9 alla somma delle sue cifre.

Da cui segue anche il criterio di divisibilità per 9: ***"un numero è divisibile per*** 9 ***se e solo se lo è la somma delle sue cifre"***.

Per quanto riguarda il metodo delle cifre, analogamente al caso di $\mathbb{Z}_3$:

In $\mathbb{Z}_9$, cambiando l'ordine delle cifre di un numero (o anche eliminando le cifre nulle oppure cifre / gruppi di cifre multipli di 9), si ottiene un numero equivalente a quello iniziale.

Esempio 6 (continuazione) *Se* $m = 427831$ *fosse divisibile per* 9 *allora sarebbe divisibile anche per* 3, *ma sappiamo già dall'Esempio 6 che non lo è. Cerchiamo allora il numero divisibile per* 9 *più vicino a* m.
Riducendo 427831 *modulo* 9, *si ha*

$$m = 427831 = 4 + 2 + 7 + 8 + 3 + 1 \ (\textit{mod}\ 9) = 25 \ (\textit{mod}\ 9) = 2 + 5 \ (\textit{mod}\ 9) = 7 \ (\textit{mod}\ 9)$$

ed essendo il resto della divisione di m *per* 9 *pari a* 7, *il numero divisibile per* 9 *più vicino a* m *si ottiene sommando* 2 *a* m, *dunque* 427833.
Un modo estremamente rapido per calcolare la riduzione di 427831 *modulo* 9 *è, impiegando il metodo delle cifre, il seguente:*

$$m = 427831 \overset{(a)}{=} 812743 \ (\textit{mod}\ 9) \overset{(b)}{=} 43 \ (\textit{mod}\ 9) = 7 \ (\textit{mod}\ 9)\,,$$

dove nell'uguaglianza (a) abbiamo riordinato le cifre e nell'uguaglianza (b) abbiamo eliminato i gruppi di cifre 81 *e* 27 *in quanto equivalenti a* 0 *modulo* 9.

2.3.3 Riduzione modulo 4 e modulo 8

Riduzione modulo 4
Cominciamo con la riduzione modulo 4 di 10 e delle sue potenze (metodo base):

$$\begin{cases} 10 = 2 \pmod 4 \\ 10^2 = 2^2 \pmod 4 = 0 \pmod 4 \\ 10^3 = 10 \cdot 10^2 \pmod 4 = 2 \cdot 0 \pmod 4 = 0 \pmod 4 \\ \text{iterando, } \forall\, h \in \mathbb{N}\,,\ h \geq 2\,,\ 10^h = 10^{h-2} \cdot 10^2 \pmod 4 = 10^{h-2} \cdot 0 \pmod 4 = 0 \pmod 4\,, \end{cases}$$

ossia, **a partire da 10^2 tutte le potenze di 10 sono equivalenti a 0 modulo 4.**
Conseguentemente, usando il metodo base, il problema della riduzione modulo 4 può essere risolto come illustrato negli esempi seguenti:

$$\begin{aligned} m = 93 = \ & 9 \cdot 10 + 3 \pmod 4 \overset{\text{(b)}}{=} \\ = \ & 9 \cdot 2 + 3 \pmod 4 = 21 \pmod 4 = 1 \pmod 4\,; \end{aligned}$$

$$\begin{aligned} m = 75374 = \ & 7 \cdot 10^4 + 5 \cdot 10^3 + 3 \cdot 10^2 + 7 \cdot 10 + 4 \pmod 4 \overset{\text{(b)}}{=} \\ = \ & 7 \cdot 0 + 5 \cdot 0 + 3 \cdot 0 + 7 \cdot 2 + 4 \pmod 4 = \\ = \ & 18 \pmod 4 = 2 \pmod 4\,, \end{aligned}$$

dove nelle uguaglianze (b) abbiamo sostituito il 10 con 2 e le potenze di 10 dalla seconda in su con 0 in virtù delle equivalenze ricavate sopra. Quindi, poiché le potenze di 10 con esponente maggiore o uguale a 2 sono del tutto ininfluenti ai fini della riduzione modulo 4, si ha che

> Ogni numero positivo è equivalente modulo 4 al numero che si ottiene considerando solo le sue ultime due cifre (ossia, la cifra delle decine e quella delle unità).

Da cui segue anche il criterio di divisibilità per 4: **"*un numero è divisibile per 4 se e solo se lo è il numero costituito dalle sue ultime due cifre*"**.
La riduzione modulo 4 viene ulteriormente semplificata se, al metodo base, si combina il metodo delle cifre:

$$m = 93 \overset{\text{(c)}}{=} 13 \pmod 4 = 1 \pmod 4\,;$$

$$m = 75374 = 74 \pmod 4 \overset{\text{(d)}}{=} 30 \pmod 4 = 2 \pmod 4\,,$$

dove nell'uguaglianza (c) si usa il fatto che 9 è equivalente a 1 modulo 4 e, nell'uguaglianza (d), il fatto che 7 e 4 sono equivalenti, rispettivamente, a 3 e 0 modulo 4.

Esempio 7 *In $\mathbb{Z}_4$, calcolare il risultato del prodotto $m \cdot p$, dove $m = 350763$ e $p = 3654$.*
La richiesta corrisponde a determinare la riduzione modulo 4 del prodotto $m \cdot p$. A tal fine non è necessario (ed anzi, è sconsigliato) svolgere il prodotto $m \cdot p$, si può equivalentemente

prima ridurre i due fattori e successivamente eseguire il prodotto tra i numeri (piccoli) ottenuti. Riducendo m *e* p *modulo* 4*, si ha*

$$\begin{aligned} m = 350763 = &\quad 63 \ (\textit{mod}\ 4) = 23 \ (\textit{mod}\ 4) = 3 \ (\textit{mod}\ 4) \\ p = 3654 = &\quad 54 \ (\textit{mod}\ 4) = 10 \ (\textit{mod}\ 4) = 2 \ (\textit{mod}\ 4)\,, \end{aligned}$$

quindi

$$m \cdot p = 350763 \cdot 3654 \ (\textit{mod}\ 4) = 3 \cdot 2 \ (\textit{mod}\ 4) = 6 \ (\textit{mod}\ 4) = 2 \ (\textit{mod}\ 4)\,.$$

Riduzione modulo 8

Per quanto riguarda la riduzione modulo 8 di 10 e delle sue potenze (metodo base) , si ha:

$$\begin{cases} 10 = 2 \ (\text{mod}\ 8) \\ 10^2 = 2^2 \ (\text{mod}\ 8) = 4 \ (\text{mod}\ 8) \\ 10^3 = 2^3 \ (\text{mod}\ 8) = 0 \ (\text{mod}\ 8) \\ \forall\, h \in \mathbb{N}\,,\ h \geq 3\,,\ 10^h = 10^{h-3} \cdot 10^3 \ (\text{mod}\ 8) = 10^{h-3} \cdot 0 \ (\text{mod}\ 8) = 0 \ (\text{mod}\ 4)\,, \end{cases}$$

ossia, **a partire da** 10^3 **tutte le potenze di** 10 **sono equivalenti a** 0 **modulo** 8. Quindi,

Ogni numero positivo è equivalente modulo 8 al numero che si ottiene considerando solo le sue ultime tre cifre (ossia, le cifre delle centinaia, delle decine e delle unità).

Questo fatto, combinato con il metodo delle cifre, rende immediata la riduzione modulo 8 come illustrato negli esempi seguenti:

$$\begin{aligned} m = 93 &\overset{(a)}{=} \ 13 \ (\text{mod}\ 8) = 5 \ (\text{mod}\ 8)\,; \\ m = 75374 = &\ \ 374 \ (\text{mod}\ 8) \overset{(b)}{=} 54 \ (\text{mod}\ 8) = 6 \ (\text{mod}\ 8)\,, \end{aligned}$$

dove nell'uguaglianza (a) abbiamo sostituito la cifra 9 con 1 e nell'uguaglianza (b) abbiamo sostituito il gruppo di cifre 37 con 5 $\big($perché $37 = 5 \ (\text{mod}\ 8)\big)$.
Fermo restando che il modo più semplice per stabilire se un dato numero m è divisibile per 8 consiste nel ridurre m modulo 8 e vedere se il risultato è 0, da quanto visto finora possiamo comunque far discendere un facile criterio di divisibilità per 8. ***"Un numero*** m ***è divisibile per*** 8 ***se e solo se il numero*** q ***costituito dalle sue ultime due cifre è divisibile per*** 4 ***e, allo stesso tempo, vale la seguente ulteriore proprietà:***

- ***(a) se*** q ***è anche divisibile per*** 8***, la cifra delle centinaia è pari;***
- ***(b) se*** q ***non è divisibile per*** 8***, la cifra delle centinaia è dispari"***.

Esempio 8

- 534 *non è divisibile per* 8 *perché non è divisibile per* 4 *(*34 *non è divisibile per* 4*);*

- 528 *è divisibile per* 8 *perché:* 28 *è divisibile per* 4 *ma non per* 8 *e la cifra delle centinaia è dispari; similmente,* 836 *non è divisibile per* 8 *(*36 *è divisibile per* 4 *ma non per* 8 *e la cifra delle centinaia è pari);*

- 324 *non è divisibile per* 8 *perché* 24 *è divisibile per* 4 *e per* 8 *e la cifra delle centinaia è dispari;* 672 *è divisibile per* 8 *(*72 *è divisibile per* 4 *e per* 8 *e la cifra delle centinaia è pari);*

Per capire l'origine di tale criterio, osserviamo dapprima che se un numero m è divisibile per 8 allora lo è anche per 4 (ossia, se non è divisibile per 4 non lo è neppure per 8) e ciò spiega la necessità che il numero q costituito dalle ultime due cifre di m sia divisibile per 4. Inoltre, indicata con c la cifra delle centinaia, il numero m si riscrive come

$$m = c \cdot 10^2 + q \ :$$

se q è divisibile per 8, allora dà contributo nullo alla riduzione modulo 8 di m (ossia, conta solo la cifra c delle centinaia) e, ricordando che $10^2 = 4 \pmod 8$, è necessario che c sia pari affinché, moltiplicata per 4, dia un numero equivalente a 0 modulo 8; simmetricamente, se invece q è divisibile per 4 ma non per 8, allora q dà contributo 4 alla riduzione modulo 8 di m $\big(q = 4 \pmod 8\big)$ e occorre che c sia dispari affinché la cifra delle centinaia dia un ulteriore contributo equivalente a 4 modulo 8 $\big($cosicché $4 + 4 = 0 \pmod 8\big)$.

2.3.4 Riduzione modulo 5 e modulo 10

Riduzione modulo 5
Poiché $10 = 0 \pmod 5$, tutte le potenze di 10 sono equivalenti a 0 modulo 5 e la riduzione modulo 5 si effettua semplicemente riducendo modulo 5 la cifra delle unità:

$$m = 24728 = 8 \pmod 5 = 3 \pmod 5 .$$

Riduzione modulo 10
Dato che $10 = 0 \pmod{10}$, la riduzione modulo 10 è data direttamente dalla cifra delle unità:

$$m = 24728 = 8 \pmod{10} .$$

Esempio 9 *Calcola la cifra finale del prodotto* $m \cdot p$*, dove* $m = 5943$ *e* $p = 67538$*.*
La richiesta corrisponde a determinare la riduzione modulo 10 *del prodotto* $m \cdot p$*. Come già visto nell'Esempio 7, a tal fine è sufficiente ridurre i due fattori modulo* 10 *e poi eseguire il prodotto tra i numeri ottenuti. Si ha:*

$$m = 5943 = 3 \ (\textit{mod}\ 10) \quad \textit{e} \quad p = 67538 = 8 \ (\textit{mod}\ 10) ,$$

quindi

$$m \cdot p = 5943 \cdot 67538 \,(\textit{mod}\ 10) = 3 \cdot 8 \,(\textit{mod}\ 10) = 24 \,(\textit{mod}\ 10) = 4 \,(\textit{mod}\ 10)\,,$$

ossia il risultato del prodotto $m \cdot p$ *è un numero che finisce per* 4*.*

2.3.5 Riduzione modulo 6

Abbiamo già mostrato alcuni risultati riguardanti la riduzione modulo 6 nell'Esempio 5. Integriamo la presentazione completando il metodo base e aggiungendo un'osservazione sul metodo delle cifre. Riguardo alla riduzione delle potenze di 10, si ha:

$$\begin{cases} 10 = 4 \ (\text{mod}\ 6) \\ 10^2 = 4^2 \ (\text{mod}\ 6) = 4 \ (\text{mod}\ 6) \\ 10^3 = 10 \cdot 10^2 \ (\text{mod}\ 6) = 4 \cdot 4 \ (\text{mod}\ 6) = 4 \ (\text{mod}\ 6) \\ \text{iterando,} \forall\, h \in \mathbb{N}\,,\ h \geq 1\,,\ 10^h = 4 \ (\text{mod}\ 6)\,, \end{cases}$$

ossia, **a partire da** 10^1 **tutte le potenze di** 10 **sono equivalenti a** 4 **modulo** 6. Questo fatto ha una conseguenza interessante riguardante il metodo delle cifre cosicché in $\mathbb{Z}_6$ vale la seguente proprietà: poiché tutte le potenze di 10 tranne 10^0 (che corrisponde alla cifra delle unità) sono tra loro equivalenti modulo 6, la posizione delle cifre diverse dalla cifra delle unità è ininfluente ai fini della riduzione di un numero. Dunque,

> In $\mathbb{Z}_6$, lasciando fissa la cifra delle unità e cambiando l'ordine delle altre cifre di un numero (o anche eliminando le cifre nulle oppure cifre / gruppi di cifre multipli di 6 – pur di non modificare la cifra delle unità), si ottiene un numero equivalente a quello iniziale.

Esempio 10 *Ridurre modulo* 6 *i numeri* $m = 1488327$ *e* $p = 7543$*.*
Possiamo, ad esempio, procedere come segue:

$$m = 1488327 \overset{(a)}{=} 1248387 \,(\textit{mod}\ 6) \overset{(b)}{=} 21 \,(\textit{mod}\ 6) = 3 \,(\textit{mod}\ 6)$$

dove nell'uguaglianza (a) abbiamo lasciato ferma la cifra delle unità e riordinato le altre cifre in modo da ottenere due gruppi di cifre divisibili per 6 *(ossia,* 12 *e* 48*) e, per le due cifre rimanenti (*8 *e* 3*), fra l'ordine che dà la scrittura* 38 *e quello che dà* 83*, abbiamo scelto il primo perché* 38 *è più piccolo e quindi più facile da trattare; nell'uguaglianza (b) abbiamo ridotto modulo* 6 *i gruppi di cifre* 12 *e* 48 *(sostituendoli con* 0*), il gruppo* 38 *(sostituendolo con* 2*) e la cifra delle unità* 7 *(sostituendola con* 1*). Similmente, per* p *si ha:*

$$p = 7543 \overset{(c)}{=} 13 \,(\textit{mod}\ 6) = 1 \,(\textit{mod}\ 6)$$

dove nell'uguaglianza (c) abbiamo sostituito la cifra 7 *con* 1 *ed eliminato il gruppo* 54*.*

Osserviamo infine che, poiché 6 si scompone in fattori primi come $2 \cdot 3$, ***"un numero è divisibile per*** 6 ***se e solo se è divisibile sia per*** 2 ***che per*** 3 ***"***.

2.3.6 Riduzione modulo 7

Circa la riduzione delle potenze di 10 (metodo base), si ha:

$$\begin{cases} 10 = 3 \ (\text{mod } 7) \\ 10^2 = 3^2 \ (\text{mod } 7) = 2 \ (\text{mod } 7) \\ 10^3 = 10 \cdot 10^2 \ (\text{mod } 7) = 3 \cdot 2 \ (\text{mod } 7) = 6 \ (\text{mod } 7) \\ 10^4 = 10 \cdot 10^3 \ (\text{mod } 7) = 3 \cdot 6 \ (\text{mod } 7) = 4 \ (\text{mod } 7) \\ 10^5 = 10 \cdot 10^4 \ (\text{mod } 7) = 3 \cdot 4 \ (\text{mod } 7) = 5 \ (\text{mod } 7) \\ 10^6 = 10 \cdot 10^5 \ (\text{mod } 7) = 3 \cdot 5 \ (\text{mod } 7) = 1 \ (\text{mod } 7) \\ 10^7 = 10 \cdot 10^6 \ (\text{mod } 7) = 3 \cdot 1 \ (\text{mod } 7) = 3 \ (\text{mod } 7) \end{cases}$$

e, chiaramente, la successione procede in modo periodico ripetendo la sequenza

$$3 \to 2 \to 6 \to 4 \to 5 \to 1 \, .$$

Un esempio di riduzione modulo 7 usando il metodo delle cifre è già stato illustrato nell'Osservazione 4 dell'Esempio 5. È comunque opportuno ribadire che, in $\mathbb{Z}_7$, non c'è la libertà di cambiare l'ordine delle cifre perché, in generale, le potenze di 10 non sono tra loro equivalenti modulo 7 (e quindi la posizione di ogni cifra è importante perché a posizione diversa corrisponde una diversa potenza di 10 per cui la cifra è moltiplicata).

Esempio 11 *Applica il metodo combinato (metodo base e metodo delle cifre insieme) per ridurre modulo* 7 *il numero* $m = 465896$*.*
Si ha:

$$\begin{aligned} m = 465896 = & \ 4 \cdot 10^5 + 6 \cdot 10^4 + 5 \cdot 10^3 + 8 \cdot 10^2 + 9 \cdot 10 + 6 \ (\textit{mod } 7) = \\ = & \ 4 \cdot 5 + 6 \cdot 4 + 5 \cdot 6 + 1 \cdot 2 + 2 \cdot 3 + 6 \ (\textit{mod } 7) = \\ = & \ 20 + 24 + 30 + 2 + 6 + 6 \ (\textit{mod } 7) \overset{(a)}{=} \\ = & \ 6 + 3 + 2 + 2 + 6 + 6 \ (\textit{mod } 7) = 25 \ (\textit{mod } 7) = 4 \ (\textit{mod } 7) \, , \end{aligned}$$

dove nell'uguaglianza (a) abbiamo ridotto modulo 7 *i singoli addendi. Nota che, al fine di mantenere piccoli il più possibile i numeri con cui fare i calcoli, anziché* 4*,* 5 *e* 6 *possiamo usare, rispettivamente,* -3*,* -2 *e* -1 *(loro equivalenti modulo* 7*), quindi:*

$$\begin{aligned} m = 465896 = & \ 4 \cdot 10^5 + 6 \cdot 10^4 + 5 \cdot 10^3 + 8 \cdot 10^2 + 9 \cdot 10 + 6 \ (\textit{mod } 7) = \\ = & \ -3 \cdot (-2) - 1 \cdot (-3) - 2 \cdot (-1) + 1 \cdot 2 + 2 \cdot 3 - 1 \ (\textit{mod } 7) = \\ = & \ 6 + 3 + 2 + 2 + 6 - 1 \ (\textit{mod } 7) = 18 \ (\textit{mod } 7) = 4 \ (\textit{mod } 7) \, . \end{aligned}$$

I criteri di divisibilità per 7 sono piuttosto contorti, poco efficienti e di difficile memorizzazione. Nella pratica, riteniamo che il modo più semplice per vedere se un numero è divisibile per 7 sia quello di ridurlo modulo 7 impiegando al meglio le varie tecniche introdotte.

2.3.7 Riduzione modulo 11

Nel caso di $\mathbb{Z}_{11}$, l'uso di numeri negativi equivalenti rende il metodo base particolarmente interessante, infatti si ha:

$$\begin{cases} 10 = -1 \pmod{11} \\ 10^h = (-1)^h \pmod{11} \end{cases}$$

ossia, **le potenze di 10 ad esponente pari sono equivalenti a 1 e quelle a esponente dispari sono equivalenti a -1 modulo 11.**
Ad esempio:

$$\begin{aligned} m = 53724 = &\ 5 \cdot 10^4 + 3 \cdot 10^3 + 8 \cdot 10^2 + 2 \cdot 10 + 4 \pmod{11} = \\ = &\ 5 \cdot 1 + 3 \cdot (-1) + 8 \cdot 1 + 2 \cdot (-1) + 4 \pmod{11} = \\ = &\ 5 - 3 + 7 - 2 + 4 \pmod{11} = \\ = &\ 11 \pmod{11} = 0 \pmod{11}, \end{aligned}$$

ossia m è divisibile per 11. Possiamo cioè affermare che

> Ogni numero positivo è equivalente modulo 11 alla differenza tra la somma delle sue cifre in posizione "dispari" e la somma tra quelle in posizione "pari" (contando le posizioni da destra verso sinistra).

Da quanto visto segue anche il ben noto criterio di divisibilità per 11, ossia: ***"un numero è divisibile per 11 se e solo se lo è la differenza tra la somma delle sue cifre in posizione dispari e la somma tra quelle in posizione pari"***.

2.4 Il reciproco in $\mathbb{Z}_n$ e la funzione ϕ di Eulero

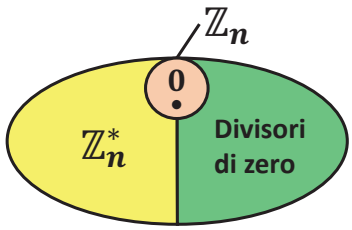


Figura 5: Ogni insieme $\mathbb{Z}_n$ si ripartisce in tre sottoinsiemi: l'elemento nullo, il sottoinsieme $\mathbb{Z}_n^*$ degli elementi invertibili e il sottoinsieme dei divisori di zero.

• RECIPROCO degli elementi di $\mathbb{Z}_n$

Def: Il RECIPROCO di un numero è quel numero che moltiplicato per il numero dato dà 1.

Esempio: In $\mathbb{Z}_9$

Il reciproco di 2 è 5 perché $2 \cdot 5 = 10 \pmod 9 = 1 \pmod 9$

di 8 è 8 perché $8 \cdot 8 = 64 \,(9) = 1 \pmod 9$

oppure $8 \cdot 8 = (-1) \cdot (-1) \pmod 9 = 1 \,(9)$

di 3 NON ESISTE perché nessun multiplo di 3 può dare resto 1 quando diviso per 9

I numeri di $\mathbb{Z}_n$ che hanno reciproco si chiamano "elementi invertibili" di $\mathbb{Z}_n$ e sono i numeri m tali che $MCD(m, n) = 1$ (ossia, sono i numeri m COPRIMI con n), tale insieme si indica con $\mathbb{Z}_n^*$.

Esempio: I numeri che hanno reciproco in $\mathbb{Z}_{12}$ sono $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

Operativamente: la ricerca del reciproco di un numero si fa direttamente dentro l'insieme $\mathbb{Z}_n^*$ e, sostanzialmente, si tratta di accoppiare tra loro gli elementi di $\mathbb{Z}_n^*$ (per alcuni numeri il reciproco è se stesso)

Esempio: Determiniamo gli elementi invertibili di $\mathbb{Z}_{14}$ e di ognuno troviamo il reciproco: $\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$

a) Il reciproco di 1 è 1 e il reciproco di 13 è 13 $\left(13 \cdot 13 = (-1) \cdot (-1) \pmod{14} = 1 \,(14)\right)$

b) Il reciproco di 3 è uno degli elementi rimasti (3 stesso, 5, 9 oppure 11):
si vede subito che è 5 $\left(3 \cdot 5 = 15 \pmod{14} = 1 \,(14)\right)$

c) Il reciproco di 9 può essere solo 9 oppure 11 (gli unici elementi rimasti)
ed è 11 (sia perché $9 \cdot 11 = 99 \,(14) = 98 + 1 \,(14) = 1 \,(14)$ perché 98 è divisibile per 14, oppure — per esclusione — non è 9 perché $9 \cdot 9 = 81 \,(14) = 80 + 1 \,(14)$ ma 80 non è divisibile per 7 e quindi neppure per 14).

DIVISORI DI ZERO: un elemento $K \neq 0$ di $\mathbb{Z}_n$ si chiama divisore di zero se esiste un elemento $h \neq 0$ in $\mathbb{Z}_n$ tale che $K \cdot h = 0 \pmod n$ [e quindi anche h è un div. di 0]

Esempio: In $\mathbb{Z}_{14}$, 2 è un divisore di 0 perché

$2 \cdot 7 = 0 \pmod{14}$ [dunque anche 7 è un div. di 0]

4 è un divisore di 0 perché $4 \cdot 7 = 0 \pmod{14}$

In $\mathbb{Z}_{16}$, 4 è un divisore di 0 perché $4 \cdot 4 = 0 \pmod{16}$

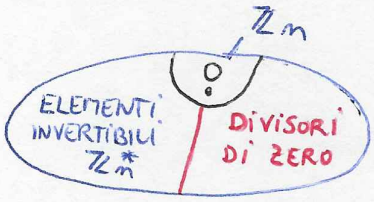
In $\mathbb{Z}_{12}$, 9 è un divisore di 0 perché $9 \cdot 4 = 0 \pmod{12}$

FATTO: se K in $\mathbb{Z}_n$ è un divisore di 0 allora K non è invertibile

~~viceversa~~ ossia, se h in $\mathbb{Z}_n$ è invertibile allora h non è un div. di 0

e, viceversa, se k non è invertibile e non è nullo, allora è un divisore di zero

QUINDI ogni insieme $\mathbb{Z}_n$ si tripartisce come in figura:



OSS. 1: se $n = p$, numero primo, tutti gli elementi di $\mathbb{Z}_p$ (esclusi solo lo 0) sono invertibili: $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$

Dunque in $\mathbb{Z}_p$ non ci sono divisori di zero.

EQUAZIONI Generalizzazione del "secondo principio di equivalenza per le equazioni": MOLTIPLICANDO AMBO I MEMBRI DI UN'EQUAZIONE PER UN ELEMENTO INVERTIBILE SI OTTIENE UN'EQUAZIONE EQUIVALENTE.

Esempio: Equazioni di primo grado in $\mathbb{Z}_n$

In $\mathbb{Z}_9$: $2X = 7$ moltiplico ambo i membri per il reciproco di 2, ossia 5, $5 \cdot 2 X = 7 \cdot 5 \to X = 35 = 8 \pmod 9$ $S = \{8\}$ ($5 \cdot 2 = 1$)

In $\mathbb{Z}_{12}$: $7X = 3$ il rec. di 7 è 7: $7 \cdot 7X = 3 \cdot 7 \to X = 21 = 9 \ (12)$ $S = \{9\}$ ($7 \cdot 7 = 1$)

Se il coefficiente di X non sta in $\mathbb{Z}_n^*$ il problema è più complicato ...

• Il TEOREMA di Eulero - Fermat

Il numero di elementi di $\mathbb{Z}_n^*$ (ossia, il numero di elementi invertibili in $\mathbb{Z}_n$) si indica con Φ_n (Φ si chiama FUNZIONE di Eulero)

Esempio: $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$, quindi $\Phi_{12} = 4$

$\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$, quindi $\Phi_{14} = 6$

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, quindi $\Phi_7 = 6$

FATTI:

1) Tranne il caso $n = 2$ ($\Phi_2 = 1$), Φ_n è sempre un numero PARI

2) Calcoliamo Φ_n nei seguenti casi:

   a) Se n è piccolo (elenca gli elementi di $\mathbb{Z}_n^*$ e contali)

   b) Se $n = p$ è primo: $\Phi_p = p - 1$ (vedi OSS. 1)

   c) Se $n = p \cdot q$ p, q primi distinti, $\Phi_n = (p-1)(q-1)$

DEF: NUMERI LIBERI DA QUADRATI

I numeri la cui scomposizione in fattori primi è fatta di fattori aventi TUTTI esponente 1 si dicono LIBERI DA QUADRATI

Esempi: $6 = 2 \cdot 3$ è libero da quadrati
$10 = 2 \cdot 5$ " "
$30 = 2 \cdot 3 \cdot 5$ " "

$4 = 2^2$ NON È libero da quadrati
$8 = 2^3$ " " "
$12 = 2^2 \cdot 3$ " " "

TEOREMA DI Eulero - Fermat:

(1) QUALUNQUE SIA n E QUALUNQUE ELEMENTO a INVERTIBILE DI $\mathbb{Z}_n$ SI PRENDA, OSSIA, QUALUNQUE SIA $a \in \mathbb{Z}_n^*$,

SI HA $$a^{\phi_n + 1} = a \pmod n \qquad (1)$$

(2) SE n È LIBERO DA QUADRATI, ALLORA L'EQUAZIONE (1) VALE PER QUALSIASI ELEMENTO DI $\mathbb{Z}_n$ (NON SOLO PER GLI INVERTIBILI)

Esempi:
- In $\mathbb{Z}_{12}$, si ha $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ e $\phi_{12} = 4$, dunque

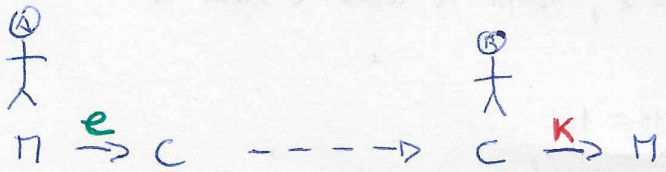
Caso (1):
- $1^5 = 1 \pmod{12}$ [ovvio];
- $5^5 = 5 \pmod{12}$ [INFATTI, $5^5 = 5^2 \cdot 5^2 \cdot 5 = \underbrace{25 \cdot 25}_{25 = 1 \pmod{12}} \cdot 5 = 1 \cdot 1 \cdot 5 = 5 \pmod{12}$]
- ed anche $7^5 = 7 \pmod{12}$; $11^5 = 11 \pmod{12}$

Invece $2^5 = 32 = 8 \mod(12) \neq 2 \pmod{12}$: infatti $2 \notin \mathbb{Z}_{12}^*$ E 12 NON È LIBERO DA QUADRATI

- In $\mathbb{Z}_6$, si ha $\mathbb{Z}_6^* = \{1, 5\}$ e $\phi_6 = 2$

Caso (2):
- Poiché 6 è LIBERO DA QUADRATI, la (1) vale PER QUALSIASI ELEM. DI $\mathbb{Z}_6$
- $2^{\phi_6 + 1} = 2^3 = 2 \pmod 6$ [$2 \notin \mathbb{Z}_6^*$]
- $5^{\phi_6 + 1} = 5^3 = 25 \cdot 5 \pmod 6 = 1 \cdot 5 = 5 \pmod 6$ [$5 \in \mathbb{Z}_6^*$]

SCHEMA per le lezioni sul METODO **RSA** di cifratura



Costruzione CHIAVI: $n = p \cdot q$

$m = \phi_n = (p-1)(q-1)$

In $\mathbb{Z}_m$: $e, K \in \mathbb{Z}_m^*$ tali che $e \cdot K = 1 \pmod m$ $\begin{cases} (n,e) & \text{PUBBL.} \\ (n,K) & \text{PRIV.} \end{cases}$

Codifica / decodifica: In $\mathbb{Z}_n$: $M \mapsto C = M^e \pmod n$ [CODIFICA]

NB: l'esponente 'e' è quello del DESTINATARIO (B) e varia al variare del destinatario (quindi C dipende da (B))

$C \mapsto C^K \pmod n = M$ [DECODIFICA]

Esempio 1: $n = 22 = 2 \cdot 11 \to m = \phi_{22} = 1 \cdot 10 = 10 \to$ in $\mathbb{Z}_{10}$: $e = 7$, $K = 3$

$M = 4 \to C = 4^7 \pmod{22} = \dots$ 22, 44, 66, 88, 110, ... $4^3 = -2\ (22)$ $\dots = (4^3)^2 \cdot 4\ (22) =$

$= (-2)^2 \cdot 4\ (22) = 16 \pmod{22}$

$C = 16 \to M = 16^3 \pmod{22} = 2^{12} \pmod{22} = \dots$ $2^5 = 10\ (22)$ $\dots = (2^5)^2 \cdot 4\ (22) =$

$= 10^2 \cdot 4\ (22) = 12 \cdot 4\ (22) = 48\ (22) = 4\ (22)$!

Esempio 2: Sia (55, 7) la chiave pubblica, determina la codifica C di $M = 2$, K e decodifica

Sol: $n = 55 = 5 \cdot 11 \to m = \phi_n = 4 \cdot 10 = 40$

Il reciproco di 7 in $\mathbb{Z}_{40}$ finisce con la cifra 3 perché, se $e \cdot K = 7 \cdot K = 1\ (40)$ allora z finisce con la cifra 1, quindi il reciproco di 7 è 3, 13, 23 oppure 33 $\to$ $K = 23$

$C = M^e\ (55) = 2^7\ (55) = 2^6 \cdot 2\ (55) = 9 \cdot 2\ (55) = 18$

$M = 18^K\ (55) = 18^{23}\ (55) = \dots$ 55, 110, 165, 220, 275, 330 $18^2 = 324 = -6\ (55)$

$\dots = (18^2)^{11} \cdot 18\ (55) = (-6)^{11} \cdot 18\ (55) = -6^{11} \cdot 18\ (55) = \dots$ $6^2 = 36$; $6^3 = 216 = -4\ (55)$

$\dots = -(6^3)^3 \cdot 6^2 \cdot 18 = -(6^3)^3 \cdot \underline{6^2 \cdot 6} \cdot 3 = -(-4)^3 (-4) \cdot 3 = 4^3 \cdot (-12)\ (55) = -9 \cdot 12\ (55) =$

$= -108\ (55) = -(-2) \pmod{55} = 2\ (55)$!

Esempio 3: Sia (15, 3) la chiave pubblica e $C = 13$, rompi il codice e trova M

Sol: Per rompere il codice abbiamo 2 possibilità:

(1) $C = M^3$ $\to$ risolviamo l'equazione $13 = M^3$ (ovvio, calcoliamo $\sqrt[3]{13}$ in $\mathbb{Z}_{15}$)

(2) Cerchiamo K

Per la (1) serve la "forza bruta", seguiamo la (2): $n = 15 = 3 \cdot 5 \Rightarrow m = 2 \cdot 4 = 8$

Il reciproco di 3 in $\mathbb{Z}_8$ è 3 $\Rightarrow$ $K = 3$ e $M = C^3\ (15) = 13^3\ (15) = (-2)^3\ (15) = -8\ (15) = 7$

Esempio 4: La chiave pubblica è $(34, 13)$ e $C = 2$, rompi il codice e trova M

Sol: (1) $M^{13} = 2 \dashrightarrow$ ☹

(2) $n = 34 = 2 \cdot 17 \rightarrow m = \phi_{34} = 1 \cdot 16 = 16$

$\mathbb{Z}_{16}^* = 1, 3, 5, 7, 9, 11, 13, 15 \quad \Rightarrow \quad K = 5$

$\Rightarrow M = 2^5 (34) = 32$

Dimostrazione del funzionamento del metodo:

Dobbiamo mostrare che, posto $C = M^e (n)$, si ha $C^K = M (n)$

Calcoliamo $C^K \pmod n$:

$$C^K \pmod n = (M^e)^K \pmod n = M^{e \cdot K} \pmod n = \dots$$

$$e \cdot K = 1 \pmod m \quad \Rightarrow \quad e \cdot K = h \cdot m + 1$$

$$\dots = M^{h \cdot m + 1} (n) = M^{h \cdot m} \cdot M (n) = (M^m)^h \cdot M (n) =$$

$$= \underbrace{M^m \cdot M^m \cdots M^m \cdot M^m}_{h\text{-volte}} \cdot M (n) = \dots$$

poiché n è libero da quadrati, $M^{\phi_n + 1} = M \pmod n$ ossia $(\phi_n = m)$ $M^m \cdot M = M (n)$

$$\dots = (M^m \cdot M)(M^m \cdot M) \cdots (M^m \cdot M)(M^m \cdot M)(n) = M \pmod n \quad !$$

($M^m \cdot M = M$; $M^m \cdot M = M$; $M^m \cdot M = M$)

Perché/quando è impossibile "rompere il codice":

Occorre da ciò che è PUBBLICO, ossia (n, e) e C, non sia possibile ricostruire il valore di K o direttamente di M.

① Si ha $\boxed{C = M^e (n)}$, ossia M è la soluzione di $x^e = C$ vale a dire $\boxed{M = \sqrt[e]{C} \pmod n}$

⇒ Se n è grande (QUALCHE centinaio di cifre) è impossibile, nella pratica, calcolare la radice e-sima di C, non esiste computer in grado di farlo in tempi non biblici.

② NB: Calcolare K, ossia il reciproco di e in $\mathbb{Z}_m$, è "facile" se è noto m (anche se m è molto grande, un computer riesce facilmente ad invertire e)

⇒ per la segretezza di K occorre che m resti segreto (ovviamente, se non si conosce m è impossibile calcolare il reciproco di e in $\mathbb{Z}_m$!)

$n = p \cdot q$ e $m = (p-1)(q-1)$ ⇒ affinché m resti segreto non bisogna conoscere p e q ⇒ se n è grande, è praticamente impossibile ricavare p e q dalla conoscenza di n

2.5 Il "Teorema di Eulero-Fermat"

Definizione 1 (Interi liberi da quadrati) *Un numero* $n \in \mathbb{N}$ *si dice essere* libero da quadrati *se nella sua scomposizione in fattori primi tutti gli esponenti sono uguali a 1*

Esempio 12 *Sono liberi da quadrati:*

- *Tutti i numeri primi*
- $n = 6$, *perché* $6 = 2 \cdot 3$
- $n = 10$, *perché* $10 = 2 \cdot 5$
- $n = 30$, *perché* $30 = 2 \cdot 3 \cdot 5$

Non sono liberi da quadrati:

$$++++$$

Se $a \in \mathbb{Z}_n^*$ allora

$$a^{\Phi_n+1} = a \pmod{n}$$

Se n è libero da quadrati, allora l'equazione di Eulero-Fermat è vera per tutti gli elementi di $\mathbb{Z}_n$: Se $a \in \mathbb{Z}_n$ allora

$$a^{\Phi_n+1} = a \pmod{n}$$

3 Esercizi

NOTA BENE: A meno che non venga richiesto esplicitamente di farne uso, tutti gli esercizi devono essere risolti **senza** usare la calcolatrice. La calcolatrice può essere utilizzata al termine dello svolgimento per verificare la correttezza del risultato.

3.1 Testo

Esercizio 1 *Determina la riduzione modulo* n *dei seguenti numeri:*

$23 =$ ___ (*mod* 2)	$38 =$ ___ (*mod* 2)	$43 =$ ___ (*mod* 3)	$39 =$ ___ (*mod* 3)
$53 =$ ___ (*mod* 3)	$31 =$ ___ (*mod* 4)	$42 =$ ___ (*mod* 4)	$37 =$ ___ (*mod* 4)
$48 =$ ___ (*mod* 4)	$56 =$ ___ (*mod* 5)	$53 =$ ___ (*mod* 6)	$73 =$ ___ (*mod* 6)
$46 =$ ___ (*mod* 6)	$84 =$ ___ (*mod* 6)	$53 =$ ___ (*mod* 7)	$75 =$ ___ (*mod* 7)
$46 =$ ___ (*mod* 8)	$84 =$ ___ (*mod* 8)	$53 =$ ___ (*mod* 8)	$75 =$ ___ (*mod* 8)
$45 =$ ___ (*mod* 9)	$75 =$ ___ (*mod* 9)	$53 =$ ___ (*mod* 10)	$176 =$ ___ (*mod* 10)
$46 =$ ___ (*mod* 11)	$121 =$ ___ (*mod* 11)	$53 =$ ___ (*mod* 12)	$53 =$ ___ (*mod* 13)
$40 =$ ___ (*mod* 14)	$75 =$ ___ (*mod* 15)	$80 =$ ___ (*mod* 17)	$99 =$ ___ (*mod* 19)
$95 =$ ___ (*mod* 60)	$206 =$ ___ (*mod* 60)	$450 =$ ___ (*mod* 360)	$500 =$ ___ (*mod* 365)

Esercizio 2 *Determina la riduzione modulo n dei seguenti numeri:*

$-17 =$ ___ (*mod* 2)	$-26 =$ ___ (*mod* 2)	$5 =$ ___ (*mod* 3)	$-5 =$ ___ (*mod* 3)
$13 =$ ___ (*mod* 3)	$-13 =$ ___ (*mod* 3)	$11 =$ ___ (*mod* 4)	$-11 =$ ___ (*mod* 4)
$16 =$ ___ (*mod* 5)	$-16 =$ ___ (*mod* 5)	$14 =$ ___ (*mod* 6)	$-14 =$ ___ (*mod* 6)
$15 =$ ___ (*mod* 6)	$-15 =$ ___ (*mod* 6)	$-23 =$ ___ (*mod* 7)	$-63 =$ ___ (*mod* 7)
$-70 =$ ___ (*mod* 8)	$-33 =$ ___ (*mod* 9)	$-13 =$ ___ (*mod* 10)	$-26 =$ ___ (*mod* 10)
$-25 =$ ___ (*mod* 10)	$-38 =$ ___ (*mod* 10)	$-1 =$ ___ (*mod* 10)	$-33 =$ ___ (*mod* 11)
$-36 =$ ___ (*mod* 11)	$-31 =$ ___ (*mod* 12)	$-34 =$ ___ (*mod* 13)	$-40 =$ ___ (*mod* 17)

Esercizio 3 *Stabilisci se le seguenti equivalenze in $\mathbb{Z}_n$ sono* **V***ere o* **F***alse:*

$83 = 29$ (*mod* 2) ☐;	$37 = 112$ (*mod* 2) ☐;	$17 = 23$ (*mod* 3) ☐;
$97 = 74$ (*mod* 3) ☐;	$93 = 38$ (*mod* 4) ☐;	$22 = 86$ (*mod* 4) ☐;
$-12 = 43$ (*mod* 5) ☐;	$64 = 22$ (*mod* 6) ☐;	$-13 = 43$ (*mod* 7) ☐;
$-25 = -45$ (*mod* 8) ☐;	$-14 = 34$ (*mod* 10) ☐;	$143 = 198$ (*mod* 11) ☐;

Esercizio 4 *Calcola le seguenti espressioni in $\mathbb{Z}_n$ giovandoti delle equivalenze modulo n.*

`Esempio:` $19 - 35 + 63 =$ ___ (*mod* 6)*;*

Soluzione: $19 - 35 + 63 = 1 - 5 + 3$ (*mod* 6) $= -1$ (*mod* 6) $= 5$ (*mod* 6)*.*

Ricorda che il risultato deve essere un elemento di $\mathbb{Z}_n = \{\, 0\,,\, 1\,,\, \ldots\, n-1\,\}$*.*

$41 + 53 + 97 =$ ___ (*mod* 2)	$34 + 18 + 28 =$ ___ (*mod* 3)	$27 - 39 + 45 =$ ___ (*mod* 4)
$59 + 48 + 84 =$ ___ (*mod* 5)	$66 + 40 + 57 =$ ___ (*mod* 6)	$67 - 18 - 50 =$ ___ (*mod* 7)
$55 + 29 + 75 =$ ___ (*mod* 8)	$94 - 58 - 17 =$ ___ (*mod* 10)	$45 + 38 + 28 =$ ___ (*mod* 12)
$50 + 48 - 20 =$ ___ (*mod* 13)	$42 - 80 - 72 =$ ___ (*mod* 16)	$49 + 65 + 86 =$ ___ (*mod* 25)

Esercizio 5 *Usa il metodo base per calcolare la riduzione modulo n dei seguenti numeri:*

$5824 =$ ___ (*mod* 3)	$7361 =$ ___ (*mod* 4)	$93198 =$ ___ (*mod* 4)
$2150 =$ ___ (*mod* 6)	$7361 =$ ___ (*mod* 6)	$5239 =$ ___ (*mod* 6)
$4655 =$ ___ (*mod* 7)	$7361 =$ ___ (*mod* 7)	$265842 =$ ___ (*mod* 7)
$3723 =$ ___ (*mod* 8)	$7361 =$ ___ (*mod* 8)	$265842 =$ ___ (*mod* 9)
$5148 =$ ___ (*mod* 11)	$7361 =$ ___ (*mod* 11)	$265842 =$ ___ (*mod* 11)
$5148 =$ ___ (*mod* 13)	$7361 =$ ___ (*mod* 13)	$7264 =$ ___ (*mod* 19)

Esercizio 6 *Usa il metodo delle cifre per calcolare la riduzione modulo n dei seguenti numeri (itera il metodo riducendo, se possibile, prima le singole cifre poi prosegui a gruppi):*

$5824 =$ ___ (*mod* 3)	$7361 =$ ___ (*mod* 4)	$93198 =$ ___ (*mod* 4)
$2150 =$ ___ (*mod* 6)	$7361 =$ ___ (*mod* 6)	$5239 =$ ___ (*mod* 6)
$4655 =$ ___ (*mod* 7)	$7361 =$ ___ (*mod* 7)	$265842 =$ ___ (*mod* 7)
$3723 =$ ___ (*mod* 8)	$7361 =$ ___ (*mod* 8)	$265842 =$ ___ (*mod* 9)
$5148 =$ ___ (*mod* 11)	$7361 =$ ___ (*mod* 11)	$265842 =$ ___ (*mod* 11)
$5148 =$ ___ (*mod* 13)	$7361 =$ ___ (*mod* 13)	$7264 =$ ___ (*mod* 19)

Esercizio 7 *Combina liberamente il metodo base e il metodo delle cifre per calcolare la riduzione modulo n dei seguenti numeri (per ogni numero, inventa due risoluzioni differenti e, in almeno una delle due, usa anche il metodo base):*

$7295 =$ ___ (*mod* 4)	$57822 =$ ___ (*mod* 6)	$589334 =$ ___ (*mod* 6)
$993752 =$ ___ (*mod* 7)	$57822 =$ ___ (*mod* 7)	$640337 =$ ___ (*mod* 7)
$7295 =$ ___ (*mod* 8)	$57822 =$ ___ (*mod* 8)	$318392 =$ ___ (*mod* 11)
$682744 =$ ___ (*mod* 11)	$57822 =$ ___ (*mod* 12)	$581089 =$ ___ (*mod* 12)
$741957 =$ ___ (*mod* 13)	$57822 =$ ___ (*mod* 14)	$490365 =$ ___ (*mod* 15)

Esercizio 8 *Usa il metodo delle cifre e la possibilità di riordinare le cifre per ridurre modulo n i seguenti numeri (ricorda che puoi riordinare liberamente le cifre in $\mathbb{Z}_3$ e $\mathbb{Z}_9$ mentre in $\mathbb{Z}_6$ non puoi spostare la cifra delle unità).*

`Esempio:` $8594467 =$ ___ (*mod* 3) *;*

Soluzione: $8594467 = 2201101\,(\textit{mod}\ 3) = \underbrace{1212001}_{\text{Riordinando le cifre}}\ (\textit{mod}\ 3) = 1\,(\textit{mod}\ 3)$ *.*

$834465 =$ ___ (*mod* 3)	$4425853 =$ ___ (*mod* 3)	$3755824 =$ ___ (*mod* 9)
$5167853 =$ ___ (*mod* 9)	$761483475 =$ ___ (*mod* 9)	$874425 =$ ___ (*mod* 6)
$9465583 =$ ___ (*mod* 6)	$2894217 =$ ___ (*mod* 6)	$767829434 =$ ___ (*mod* 6)

Esercizio 9 *Dato $m = 2893$, calcola la sua riduzione modulo n per tutti i valori di n compresi tra 2 e 20 (usa il metodo che preferisci, parti da $n = 20$ e procedi diminuendo n).*

Esercizio 10 ++++

Esercizio 11 *Stabilisci se i seguenti numeri sono divisibili per il numero n indicato e, se non lo sono, determina il multiplo di n più vicino al numero dato:*

$16434\,,\ \ n = 6\,;$	$59327\,,\ \ n = 7\,;$	$258014\,,\ \ n = 7\,;$
$5784\,,\ \ n = 8\,;$	$82366\,,\ \ n = 11\,;$	$519783\,,\ \ n = 11\,;$
$32139\,,\ \ n = 13\,;$	$65878\,,\ \ n = 14\,;$	$25846\,,\ \ n = 17\,.$

Esercizio 12 *Rispondi ai seguenti quesiti modellizzandoli con un'opportuna espressione dell'aritmetica modulare.*

`Esempio:` *Se adesso è primavera, che stagione sarà tra* 433 *stagioni?*
Soluzione. Usando il modello introdotto nell'Esempio 1, dobbiamo calcolare il risultato di $1+433$ *in* $\mathbb{Z}_4$*:* $1+433 = 1+33\,(\textit{mod}\ 4) = 34\,(\textit{mod}\ 4) = 2\,(\textit{mod}\ 4)$*, quindi saremo in estate.*

1. *Se oggi è Mercoledì, che giorno sarà tra* 600 *giorni? E tra* 1000 *giorni? Che giorno era* 150 *giorni fa?*

2. *La lancetta delle ore di un orologio segna le* 7*: se ripeto* 16 *volte l'operazione di mandare avanti di* 5 *ore tale lacetta, che ora segnerà dopo?*

Esercizio 13 *Usa l'aritmetica modulare per calcolare la cifra finale dei seguenti numeri:*

1. 2^{17}

2. 3^{28}

3. 6^{795}

4. $4^{13} + 4^{18} - 3^{23} + 7^{18}$

Esercizio 14 *Considera gli insiemi* $\mathbb{Z}_2$*,* $\mathbb{Z}_3$*, . . . ,* $\mathbb{Z}_{20}$ *e, per ognuno di essi:*

1. *Scrivi l'insieme* $\mathbb{Z}_n^*$ *degli elementi invertibili (ossia, elenca gli elementi che amettono reciproco in* $\mathbb{Z}_n$*) e, di ogni elemento invertibile, determina il reciproco;*

2. *Scrivi il valore di* Φ_n *(ossia, conta gli elementi invertibili);*

3. *Scrivi l'insieme dei divisori di zero e, di ognuno, scrivi un prodotto che mostra la proprietà di essere un divisore di zero;*
   `Esempio:` 2 *è un divisore di zero in* $\mathbb{Z}_4$ *perché* $2 \cdot 2 = 0\,(\textit{mod}\ 4)$*.*

4. *Dimostra che se* a *è invertibile allora* a *non è un divisore di zero.*
   *(*Suggerimento: se, per assurdo, esistesse $k \neq 0$ tale che $a \cdot k = 0\,(\text{mod}\ n)$, allora. . .*).*

Esercizio 15 *Risolvi le seguenti equazioni:*

In $\mathbb{Z}_4$:	$3x = 2$		
In $\mathbb{Z}_5$:	$3x = 2$	$4x = 3$	
In $\mathbb{Z}_6$:	$5x = 4$		
In $\mathbb{Z}_7$:	$2x = 5$	$3x = 2$	$5x = 4$
In $\mathbb{Z}_{10}$:	$9x = 4$	$3x = 2$	$5x - 4 = 1 - 2x$

Esercizio 16

1. *Scrivi la tavola pitagorica della moltiplicazione per gli insiemi* $\mathbb{Z}_2$, $\mathbb{Z}_3$, ..., $\mathbb{Z}_8$.

2. *Osserva la struttura e le simmetrie di tali tavole, in particolare: spiega perché sono simmetriche rispetto alla diagonale principale (quella che parte dall'angolo in alto a sinistra); spiega perché la diagonale principale è a sua volta simmetrica rispetto al suo centro; spiega perché l'ultima riga contiene gli elementi di* $\mathbb{Z}_n$ *posti in ordine decrescente.*
   Osserva inoltre che le righe relative agli elementi invertibili di $\mathbb{Z}_n$ *sono tutte e sole le righe che contengono, seppur in ordine differente, tutti gli elementi di* $\mathbb{Z}_n$.

3. *Usa le tavole pitagoriche per risolvere le seguenti equazioni:*

In $\mathbb{Z}_4$:	$2x = 2$	$2x = 1$	$x^2 = 0$		
In $\mathbb{Z}_5$:	$3x = 2$	$x^2 = 4$	$x^2 = 2$		
In $\mathbb{Z}_7$:	$5x = 6$	$x^2 = 2$	$x^2 = 3$		
In $\mathbb{Z}_8$:	$6x = 2$	$4x = 0$	$4x = 2$	$x^2 = 1$	$3x^2 = 4$

`Esempio:` *La tavola pitagorica in* $\mathbb{Z}_6$ *è la seguente (diversamente da quanto fatto qui di seguito, nel risolvere l'esercizio si omettano le righe e le colonne relative allo* 0*):*

$*$	*0*	*1*	*2*	*3*	*4*	*5*
0	*0*	*0*	*0*	*0*	*0*	*0*
1	*0*	1	2	3	4	5
2	*0*	2	4	0	2	4
3	*0*	3	0	3	0	3
4	*0*	4	2	0	4	2
5	*0*	5	4	3	2	1

Usando la tavola pitagorica, risolviamo le seguenti equazioni in $\mathbb{Z}_6$*:*

(a) $2x = 4$; *(b)* $x^2 = 3$; *(c)* $5x^2 = 4$.

Caso (a): $\mathcal{S} = \{2; 5\}$ *(consultando la riga relativa al* 2*, il risultato della moltiplicazione per* 2 *è* 4 *quando si moltiplica per* 2 *o per* 5*);*
Caso (b): $\mathcal{S} = \{3\}$ *(i quadrati degli elementi di* $\mathbb{Z}_6$ *si trovano sulla diagonale principale e il* 3 *compare solo in corrispondenza di* $3 * 3$*);*
Caso (c): $\mathcal{S} = \emptyset$*, l'equazione è impossibile (moltiplicando ambo i membri per il reciproco di* 5 *– cioè* 5 *stesso – l'equazione diventa* $5 \cdot 5x^2 = 5 \cdot 4$*, ossia* $x^2 = 2$*, e sulla diagonale principale il* 2 *non compare, ossia nessun numero di* $\mathbb{Z}_6$ *elevato al quadrato dà* 2*).*

Esercizio 17 *Risolvi le seguenti equazioni in* $\mathbb{Z}_{10}$*:*

1. $2x = 8$

2. $5x = 2$
3. $2x - 6 = 2 - 4x$
4. $3x - 2 = 4 - x$
5. $3(3x - 1) = x$

Esercizio 18 *Risolvi le seguenti equazioni in $\mathbb{Z}_6$ impiegando il cosiddetto "Metodo della forza bruta", ossia sostituendo uno a uno tutti gli elementi di $\mathbb{Z}_6$ al posto dell'incognita ed individuando i valori che rendono vera l'uguaglianza (puoi aiutarti con la tavola pitagorica):*

1. $x^2 + 3x - 4 = 0$
2. $2x^2 - x = 2$
3. $5x^2 + 2x = 0$
4. $x(x + 1) = 0$
5. $x^3 = 0\,;\quad x^3 = 1\,;\quad \cdots\ ;\ x^3 = 5$

Esercizio 19 *Elenca tutti i numeri interi liberi da quadrati compresi tra 2 e 50.*

Esercizio 20 *Considera gli insiemi $\mathbb{Z}_2$, $\mathbb{Z}_3$, ... $\mathbb{Z}_{16}$ e, per ognuno di essi, verifica la validità del Teorema di Eulero–Fermat (quando n non è libero da quadrati, fai vedere che esiste almeno un divisore di zero che non soddisfa l'uguaglianza asserita dal teorema).*

`Esempio:` *nel caso di $\mathbb{Z}_8$, poiché 8 non è libero da quadrati, l'uguaglianza $a^{\Phi_8+1} = a\,(mod\ 8)$ è garantita solo per gli elementi invertibili, ossia per $a \in \mathbb{Z}_8^*$. Si ha $\mathbb{Z}_8^* = \{1\,;3\,;5\,;7\}$ cosicché $\Phi_8 = 4$: verifichiamo dunque che ogni elemento a di $\mathbb{Z}_8^*$ è tale che $a^5 = a\,(mod\ 8)$.*
Per $a = 1$ è ovvio;
Per $a = 3$, si ha: $3^5 = (3^2)^2 \cdot 3\,(mod\ 8) = 1^2 \cdot 3\,(mod\ 8) = 3\,(mod\ 8)$, c.v.d.[2];
Per $a = 5$, si ha: $5^5 = (-3)^5\,(mod\ 8) = -3^5\,(mod\ 8) = -3\,(mod\ 8) = 5\,(mod\ 8)$, c.v.d.;
Per $a = 7$, si ha: $7^5 = (-1)^5\,(mod\ 8) = -1\,(mod\ 8) = 7\,(mod\ 8)$, c.v.d.
Per quanto riguarda gli altri elementi, l'uguaglianza è ovviamente soddisfatta per $a = 0$ $\big($chiaramente, per qualsiasi insieme $\mathbb{Z}_n$, si ha $0^{\Phi_n+1} = 0\,(mod\ n)\big)$; per i divisori di zero sappiamo invece che in generale l'uguaglianza non è garantita e che alcuni elementi potrebbero soddisfarla, altri no. Nel caso di $\mathbb{Z}_8$ è facile vedere che nessun divisore di zero b la soddisfa in quanto $b^5 = 0\,(mod\ 8)$, ad esempio: per $b = 2$, si ha: $2^5 = 32\,(mod\ 8) = 0\,(mod\ 8)$.

Esercizio 21 *Usa il Teorema di Eulero-Fermat per calcolare la riduzione modulo 14 dei seguenti numeri:*

1. 5^8

[2] c.v.d. = come volevasi dimostrare.

2. 3^{23}
3. 11^{19}
4. 2^{20}
5. 6^{23}
6. $9^{15} - 8^{25} + 5^{73}$

`Esempio`: *Usa il Teorema di Eulero-Fermat per calcolare la riduzione modulo* 20 *di* 7^{19}*.*
Soluzione. Poiché $\Phi_{20} = 8$ *e* $7 \in \mathbb{Z}_{20}^*$*, dal Teorema di Eulero–Fermat si ha* $7^9 = 7\,(mod\,20)$*.*
Quindi: $7^{19} = (7^9)^2 \cdot 7\,(mod\,20) = 7^2 \cdot 7\,(mod\,20) = 9 \cdot 7\,(mod\,20) = 3\,(mod\,20)$*.*

Esercizio 22 *Rispondi ai seguenti quesiti inerenti il metodo di cifratura "RSA":*

1. *Sia* $(22, 7)$ *la chiave pubblica e* $(22, 3)$ *la chiave privata.*
   (a) *Calcola la codifica* C *del messaggio* $M = 4$*, poi verifica che decodificando per mezzo della chiave privata si ottiene* M*.*
   (b) *Stesso quesito del punto precedente con* $M = 7$*.*
2. *Sia* $(55, 7)$ *la chiave pubblica.*
   (a) *Calcola la codifica* C *del messaggio* $M = 2$*, trova* k *e verifica che decodificando per mezzo della chiave privata si ottiene* M*.*
   (b) *Stesso quesito del punto precedente con* $M = 4$*.*
3. (a) *Sia* $(33, 17)$ *la chiave pubblica, calcola la codifica* C *del messaggio* $M = 2$*, trova* k *e verifica che decodificando per mezzo della chiave privata si ottiene* M*.*
   (b) *Stesso quesito del punto precedente con la chiave pubblica* $(33, 7)$ *e* $M = 3$*.*
4. *Il Sig. Verdi vuole spedire il messaggio* $M = 3$ *al Sig. Bianchi e alla Sig.ra Rossi. La chiave pubblica del Sig. Bianchi è* $(15, 3)$ *mentre la chiave pubblica della Sig.ra Rossi è* $(22, 7)$*. Calcola la codifica* C_B *del messaggio che riceve il Sig. Bianchi e la codifica* C_R *del messaggio che riceve la Sig.ra Rossi. Determina le chiavi private del Sig. Bianchi e della Sig.ra Rossi e verifica che entrambi, decodificando per mezzo della loro chiave privata, ottengono* M*.*
5. (a) *Sia* $(35, 17)$ *la chiave pubblica, e sia* $C = 20$ *il messaggio in codice. "Rompi il codice" e ricostruisci il messaggio originale* M*.*
   (b) *Stesso quesito del punto precedente con la chiave pubblica* $(34, 11)$ *e* $C = 22$*.*

3.2 Risultati

ISIS C. Facchinetti **Verifica di Matematica** (B. Picasso) 21/05/2019

Cognome: Nome: Classe: **5 AI**

Valutazione delle **competenze**. **M5:** **M7:**

Esercizio 1. Rispondi ai seguenti quesiti:

1.1- $-20 = \ldots \pmod 6$;

1.2- L'opposto di 4 in $\mathbb{Z}_{13}$ è $\ldots$;

1.3- Calcola il risultato della seguente espressione in $\mathbb{Z}_9$ (motiva la risposta): $58756 \cdot 3 \cdot 6 =$

1.4- Dire se le seguenti uguaglianze sono vere o false (motiva la risposta):

$$79 = 44 \pmod 7; \qquad 553 = 587 \pmod{36}$$

1.5- Stabilisci se i seguenti numeri sono divisibili per il numero n indicato e, se non lo sono, determina il multiplo di n più vicino al numero dato:

$$48916, \quad n = 7; \qquad 5723, \quad n = 8; \qquad 549, \quad n = 17$$

1.6- Rispondi al seguente quesito modellizzandolo con un'opportuna espressione dell'aritmetica modulare: "Il famoso whisky Stravecchio di Scozia si produce secondo il seguente rigido protocollo: in Maggio avviene la distillazione, quindi inizia una lunga procedura di invecchiamento che consta di 7 cicli, ognuno della durata di 15 mesi, in botti di vario tipo; al termine del settimo ciclo, il distillato viene trasferito per altri 20 mesi in una speciale barrique e quindi viene imbottigliato. In quale mese dell'anno avviene l'imbottigliamento?"

Esercizio 2. Risolvi le seguenti equazioni:

2.1- In $\mathbb{Z}_{11}$: $5x = 3$;

2.2- In $\mathbb{Z}_4$: $x - 1 = 1 - x$.

Esercizio 3. Considera $\mathbb{Z}_9$:

3.1- Elenca gli elementi di $\mathbb{Z}_9^*$ e determina Φ_9;

3.2- Enuncia il Teorema di Eulero–Fermat in $\mathbb{Z}_9$;

3.3- In $\mathbb{Z}_9$, calcola $4^7 + 2^{17} =$

Esercizio 4. Considera il metodo di crittografia "RSA" e la notazione usuale. Sia $n = 33$ ed $e = 7$ la chiave pubblica:

4.1- Calcola Φ_{33} e la chiave privata k;

4.2- Sia M il messaggio originale e sia $C = 8$ il messaggio codificato: determina M.

COMPITO SU
ARITMETICA MODULARE
21/05/2019 SAI

SOLUZIONI

① 1.1) $-20 = 4 \pmod 6$ 1.2) $-4 = 9 \pmod{13}$

1.3) $58756 \cdot \underbrace{3 \cdot 6}_{18} = 58 \cdot 756 \cdot 0 \pmod 9 = 0 \pmod 9$

1.4) $79 = 44 \pmod 7 \leftrightarrow 79 - 44 = 0 \pmod 7 \leftrightarrow 35 = 0 \pmod 7 \rightarrow$ VERO

$553 = 587 \pmod{36} \leftrightarrow 587 - 553 = 0 \pmod{36} \leftrightarrow 34 = 0 \pmod{36} \rightarrow$ FALSO

1.5) $48916 = \underbrace{41}_{6}\underbrace{21}_{00}6 \pmod 7 = \underbrace{6006}_{4} \pmod 7 = \underbrace{406}_{5}(7) = 56(7) = 0(7) \rightarrow$ SÍ, È DIVISIBILE

$5723 = \underbrace{723}_{00} \pmod 8 = 3 \pmod 8 \rightarrow$ NON È DIVISIBILE $\rightarrow m = 5720$

$\underbrace{549}_{3} = 39 \pmod{17} = 5 \pmod{17} \rightarrow$ NON È DIVISIBILE $\rightarrow m = 544$

$(17, 34, 51, \dots)$

1.6) In $\mathbb{Z}_{12}$: $\underset{\uparrow \text{Maggio}}{5} + 7 \cdot 15 + 20 = 5 + 7 \cdot 3 + 8 \pmod{12} = 5 + 21 + 8 \pmod{12} =$

$= 5 + 9 + 8 \,(12) = 22 \,(12) = 10 \,(12) \rightarrow$ OTTOBRE

② 2.1) In $\mathbb{Z}_{11}$: $5X = 3$ il reciproco di 5 è 9 $(5 \cdot 9 = 45(11) = 1(11))$

$\Updownarrow$

$9 \cdot 5X = 9 \cdot 3 \,(11) \leftrightarrow X = 27(11) \leftrightarrow X = 5 \qquad S = \{5\}$

2.2) In $\mathbb{Z}_4$: $X - 1 = 1 - X \leftrightarrow 2X = 2 \,(4) \leftrightarrow S = \{1; 3\}$ ($x=0$ e $x=2$ non risolvono)

③ 3.1) $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\} \rightarrow \phi_9 = 6$

3.2) 9 NON È LIBERO DA QUADRATI, quindi $\forall a \in \mathbb{Z}_9^*$, $a^7 = a \pmod 9$

3.3) $4, 2 \in \mathbb{Z}_9^*$ quindi $4^7 + 2^{17} = 4^7 + (2^7)^2 \cdot 2^3 \,(9) = 4 + 2^2 \cdot 2^3 \,(9) = 4 + 32 \,(9) = 0 \,(9$

④ 4.1) $33 = 3 \cdot 11 \rightarrow \phi_{33} = (3-1) \cdot (11-1) = 2 \cdot 10 = 20$

$K =$ reciproco di $e = 7$ in $\mathbb{Z}_{20}$, ossia $K = 3$

4.2) $M = C^K \pmod{33} = 8^3 \,(33) = 64 \cdot 8 \,(33) = -2 \cdot 8 \,(33) = -16 \,(33) = 17$

ISIS C. Facchinetti **Verifica di Matematica** (B. Picasso) /05/2019

Cognome: Nome: Classe: **5 AI**

Valutazione delle **competenze**. **M5:** **M7:**

Esercizio 1. Rispondi ai seguenti quesiti:

1.1- $-40 = \ldots \pmod{14}$;

1.2- L'opposto del reciproco di 11 in $\mathbb{Z}_{13}$ è $\ldots$;

1.3- Sia h un numero a 4 cifre. Completa h scrivendo la cifra delle unità in modo tale che il numero risulti divisibile per 11 (motiva la risposta): $h = 916\ldots$

1.4- Dire se le seguenti uguaglianze sono vere o false (motiva la risposta):

$$93 = 39 \pmod{6}; \qquad 1761 = 1829 \pmod{34}$$

1.5- Stabilisci se i seguenti numeri sono divisibili per il numero n indicato e, se non lo sono, determina il multiplo di n più vicino al numero dato:

$$57913, \quad n = 7; \qquad 31376, \quad n = 8; \qquad 547, \quad n = 23$$

1.6- Rispondi al seguente quesito modellizzandolo con un'opportuna espressione dell'aritmetica modulare: "Per curare la sindrome SMT (Skip the Maths Test), all'Istituto "C. Noiosetti" hanno stabilito una cura che prevede il seguente rigido protocollo: alle ore 11 del mattino del primo giorno si interroga lo studente sugli integrali; segue la somministrazione di una serie di esercizi obbligatori sui vari argomenti del programma di Matematica, da svolgere uno ogni 31 ore (il primo viene assegnato 31 ore dopo l'inizio dell'interrogazione), per un totale di 5 esercizi; infine, 53 ore dopo l'assegnazione dell'ultimo esercizio, lo studente deve sostenere un Test on–line. A che ora lo studente deve sostenere il test (specifica se di giorno o di notte)?"

Esercizio 2. Risolvi le seguenti equazioni:

2.1- In $\mathbb{Z}_{11}$: $8x = 4$;

2.2- In $\mathbb{Z}_9$: $2x - 1 = 2 - x$.

Esercizio 3. Considera $\mathbb{Z}_{12}$:

3.1- Elenca gli elementi di $\mathbb{Z}_{12}^*$ e determina Φ_{12};

3.2- Enuncia il Teorema di Eulero–Fermat in $\mathbb{Z}_{12}$;

3.3- In $\mathbb{Z}_{12}$, calcola $7^5 + 6^5 + 5^{10} =$

Esercizio 4. Considera il metodo di crittografia "RSA" e la notazione usuale. Sia $n = 33$ ed $e = 3$ la chiave pubblica:

4.1- Calcola Φ_{33} e la chiave privata k;

4.2- Sia M il messaggio originale e sia $C = 5$ il messaggio codificato: determina M.

ISIS C. Facchinetti **Verifica di Matematica** (B. Picasso) /05/2019

Cognome: Nome: Classe: **5 AI**

Valutazione delle **competenze**. **M5:** **M7:**

Esercizio 1. Rispondi ai seguenti quesiti:

1.1- $-40 = \ldots 2 \ldots \pmod{14}$; $(40 = 12 \pmod{14} \Rightarrow -40 = -12 \ (14) = 2 \pmod{14})$

1.2- L'opposto del reciproco di 11 in $\mathbb{Z}_{13}$ è $\ldots 7 \ldots$; (rec. di 11 = rec. di -2 = $-7 = 6$, l'opposto di 6 è 7)

1.3- Sia h un numero a 4 cifre. Completa h scrivendo la cifra delle unità in modo tale che il numero risulti divisibile per 11 (motiva la risposta): $h = 916\ldots 3 \ldots$. ($9+6-1-x = 14-x$ sia divisibile per 11)

1.4- Dire se le seguenti uguaglianze sono vere o false (motiva la risposta):

$93 = 33 \ (6) = 3$
$39 = 3 \ (6)$

$93 = 39 \pmod 6$; VERA

$1829 - 1761 = 68 = 0 \ (34)$

$1761 = 1829 \pmod{34}$ VERA

1.5- Stabilisci se i seguenti numeri sono divisibili per il numero n indicato e, se non lo sono, determina il multiplo di n più vicino al numero dato:

$57913 = 50213 \ (7) =$
$= 1003 \ (7) = 30 \ (7) =$
$= 23 \ (7) = 2 \ (7)$ → NON DIVISIBILE, $m = 57911$

57913, $n = 7$;

$31376 = 376 \ (8) =$
$= 56 \ (8) = 0$

31376, $n = 8$; DIVISIBILE

23 46 69 ...
$547 = 501 \ (23) = 21 \ (23) = 18 \ (3)$

547, $n = 23$; NON DIVISIBILE → $m = 552$

1.6- Rispondi al seguente quesito modellizzandolo con un'opportuna espressione dell'aritmetica modulare: "Per curare la sindrome SMT (Skip the Maths Test), all'Istituto "C. Noiosetti" hanno stabilito una cura che prevede il seguente rigido protocollo: alle ore 11 del mattino del primo giorno si interroga lo studente sugli integrali; segue la somministrazione di una serie di esercizi obbligatori sui vari argomenti del programma di Matematica, da svolgere uno ogni 31 ore (il primo viene assegnato 31 ore dopo l'inizio dell'interrogazione), per un totale di 5 esercizi; infine, 53 ore dopo l'assegnazione dell'ultimo esercizio, lo studente deve sostenere un Test on–line. A che ora lo studente deve sostenere il test (specifica se di giorno o di notte)?"

Esercizio 2. Risolvi le seguenti equazioni:

$11 + 5 \cdot 31 + 53 \pmod{24} = 11 + 5 \cdot 7 + 5 \ (24) =$
$= 11 + 11 + 5 \ (24) = 27 \ (24) = 3 \ (24)$
⇒ ORE 3, NOTTE!

2.1- In $\mathbb{Z}_{11}$: $8x = 4$; rec. di $8 = 7 \Rightarrow 7 \cdot 8x = 4 \cdot 7$, $x = 28 \ (11) \Rightarrow x = 6 \Rightarrow S = \{6\}$

2.2- In $\mathbb{Z}_9$: $2x - 1 = 2 - x$. [V. SOTTO]

Esercizio 3. Considera $\mathbb{Z}_{12}$:

3.1- Elenca gli elementi di $\mathbb{Z}_{12}^*$ e determina Φ_{12}; $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\} \Rightarrow \phi_{12} = 4$

3.2- Enuncia il Teorema di Eulero–Fermat in $\mathbb{Z}_{12}$; 12 NON È LIB. DA QUADRATI → $\forall a \in \mathbb{Z}_{12}^*$, $a^5 = a \pmod{12}$

3.3- In $\mathbb{Z}_{12}$, calcola $7^5 + 6^5 + 5^{10} =$ 8 (mod 12) [V. SOTTO]

Esercizio 4. Considera il metodo di crittografia "RSA" e la notazione usuale. Sia $n = 33$ ed $e = 3$ la chiave pubblica:

4.1- Calcola Φ_{33} e la chiave privata k; $33 = 3 \cdot 11 \Rightarrow \phi_{33} = (3-1)\cdot(11-1) = 2 \cdot 10 = 20$; K = rec. di 3 in $\mathbb{Z}_{20}$: $K = 7$

4.2- Sia M il messaggio originale e sia $C = 5$ il messaggio codificato: determina M.

$M = 5^7 \ (33) = 5^3 \cdot 5^3 \cdot 5 \ (33) = (-7)(-7) \cdot 5 \ (33) = 7 \cdot 35 \ (33) = 7 \cdot 2 \ (33) = 14$ $M = 14$

33, 66, 99, 132, $125 = -7 \ (33)$

2.2) $3X = 3$ in $\mathbb{Z}_9$ MULTIPLI DI 3 + 3: 3, 12, 21, 30, ... $S = \{1, 4, 7\}$

$x=1$ $x=4$ $x=7$

3.3) $7 \in \mathbb{Z}_9^*$ e $5 \in \mathbb{Z}_9^* \Rightarrow 7^5 = 7$ e $5^5 = 5$ (T. di Eul.-F.), invece $6^5 = 36 \cdot 6^3 = 0 \cdot 6^3 = 0 \pmod{12}$

$\Rightarrow 7^5 + 6^5 + 5^{10} = 7 + 0 + (5^5)^2 = 7 + 5^2 = 7 + 1 = 8 \pmod{12}$