CAPITOLO 9

Gli anelli delle classi di resto

§ 9.1 Unità e zero-divisori in $\mathbb{Z}_n$

Il risultato seguente caratterizza le unità e gli zero-divisori degli anelli $\mathbb{Z}_n$.

Proposizione 9.1. *Siano $a, n \in \mathbb{Z}$, $n \geq 2$. Allora:*

1) *$[a]$ è una unità in $\mathbb{Z}_n \iff MCD(a,n) = 1$;*

2) *$[a]$ è uno zero-divisore in $\mathbb{Z}_n \iff MCD(a,n) > 1$.*

Dimostrazione. **1)** $[a]$ è una unità in $\mathbb{Z}_n \iff \exists b \in \mathbb{Z}$ tale che $[a][b] = [ab] = [1]$ in $\mathbb{Z}_n \iff \exists b \in \mathbb{Z}$ tale che $ab - 1 \in n\mathbb{Z} \iff \exists b, t \in \mathbb{Z}$ tali che $1 = ab + nt \iff MCD(a,n)/1$ (cfr. Lemma 8.17) $\iff MCD(a,n) = 1$. **2)** $[a]$ è zero-divisore in $\mathbb{Z}_n \iff \exists [b] \in \mathbb{Z}_n$, $[b] \neq [0]$, tale che $[a][b] = [ab] = [0]$ in $\mathbb{Z}_n \iff \exists b \in \mathbb{Z}$, $0 < b < n$, tale che $ab \in n\mathbb{Z} \iff mcm(a,n) \leq ab < an \iff MCD(a,n) > 1$. □

Ricordiamo ora la definizione di campo e una proprietà valida per ogni anello commutativo con identità: Si dice che un anello commutativo con identità A è un **campo** se ogni elemento non nullo di A è una unità.

Lemma 9.2. *Sia A un anello commutativo con identità.*

i) *Se u è un elemento invertibile di A, allora u non è uno zero-divisore.*

ii) *Se A è un campo, allora A è un dominio di integrità.*

Dimostrazione. Proviamo che se u è invertibile e si ha $ub = 0_A$, allora necessariamente $b = 0_A$. Moltiplichiamo i due membri di $ub = 0_A$ per u^{-1}; si ottiene $b = 1_A \cdot b = u^{-1}ub = u^{-1} \cdot 0_A = 0_A$ ossia $b = 0_A$, come volevasi. La seconda affermazione si ottiene subito dalla prima ricordando le definizioni di campo e di dominio. □

Corollario 9.3. *Sia n un intero ≥ 2. Allora:*

$$\mathbb{Z}_n \text{è un campo} \iff \mathbb{Z}_n \text{ è un dominio} \iff n \text{ è un numero primo.}$$

Dimostrazione. "$\mathbb{Z}_n$ è un campo $\Longrightarrow$ $\mathbb{Z}_n$ è un dominio" è un caso particolare del lemma precedente. Per provare "$\mathbb{Z}_n$ è un dominio $\Longrightarrow$ n è un numero primo" basta ricordare che se n non è primo, allora è riducibile e osservare che i fattori di una sua fattorizzazione $n = ab$ corrispondono a classi $[a]$ e $[b]$ non nulle in $\mathbb{Z}_n$ ma tali che $[a][b] = [0]$ ossia a zero-divisori propri. Infine "n è un numero primo $\Longrightarrow$ $\mathbb{Z}_n$ è un campo" si ottiene ricordando che ogni classe in $\mathbb{Z}_n$ è del tipo $[r]$ con $0 \leq r < n$; se n è primo, allora per ogni classe $[r]$ non nulla, ossia tale che $0 < r < n$, si ha $MCD(r, n) = 1$ e quindi $[r]$ è invertibile in $\mathbb{Z}_n$ (Proposizione 9.1). □

Esempio 9.4. In $\mathbb{Z}_{35}$ $[16]$ è invertibile poiché $MCD(16, 35) = 1$. Per determinarne l'inverso, calcoliamo (mediante l'algoritmo euclideo) l'identità di Bézout $1 = 16 \cdot (-24) + 35 \cdot 11$. In $\mathbb{Z}_{35}$ si ha allora $[16][-24] = [1]$ e quindi $[-24] = [16]^{-1}$. Notiamo che i coefficienti dell'identità di Bézout non sono unicamente determinati; ad esempio si ha anche $1 = 16 \cdot 11 + 35 \cdot (-5)$; questo non contrasta con l'unicità dell'inverso poiché in $\mathbb{Z}_{35}$ si ha $[-24] = [11]$. In $\mathbb{Z}_{35}$ $[15]$ è uno zero-divisore, poiché $MCD(15, 35) = 5 > 1$. Si ha infatti $[15][7] = [0]$, con $[7] \neq [0]$, avendo ottenuto 7 dalla divisione $35 : MCD(15, 35)$.

§ 9.2 Congruenze

Definizione 9.5. *Una congruenza lineare è una equazione in $\mathbb{Z}$ del tipo $aX \equiv b \bmod n$, con $a, b, n \in \mathbb{Z}$. Sono soluzioni della congruenza tutti i numeri interi x tali che $ax - b$ è multiplo di n.*

Risulta evidente dalla definizione che se x è soluzione della congruenza $aX \equiv b \bmod n$, anche $x + nt$ lo è, per ogni $t \in \mathbb{Z}$. Risolvere la congruenza $aX \equiv b \bmod n$ equivale a risolvere in $\mathbb{Z}_n$ l'equazione lineare in una variabile $[a][X] = [b]$, oppure a risolvere in $\mathbb{Z} \times \mathbb{Z}$ l'equazione lineare in due variabili $aX + nY = b$. Quest'ultimo modo di interpretare una congruenza lineare ci fornisce immediatamente il criterio per sapere se ammette soluzioni e, in caso affermativo, il metodo per calcolare le soluzioni stesse.

Teorema 9.6. *La congruenza lineare $aX \equiv b \bmod n$ ammette soluzioni se e solo se $MCD(a, n)$ divide b.*

Dimostrazione. L'asserto segue immediatamente dal Corollario 8.17. □

Metodo risolutivo per le congruenze lineari. Se una congruenza lineare $aX \equiv b \bmod n$ soddisfa la condizione $MCD(a, n)/b$, possiamo dividere i coefficienti a, b, n per il $MCD(a, n)$ ottenendo una congruenza $a'X \equiv b' \bmod n'$ equivalente alla precedente (ossia con le stesse soluzioni) e tale che $MCD(a', n') = 1$. Possiamo allora supporre $MCD(a, n) = 1$. Risolviamo in $\mathbb{Z}_n$ l'equazione lineare $[a][X] = [b]$

moltiplicando i due membri per l'inverso $[c]$ di $[a]$ ($[c]$ esiste poiché $MCD(a,n)=1$ e c può essere calcolato mediante l'algoritmo euclideo). In $\mathbb{Z}_n$ vi è l'unica soluzione $[bc]$. L'insieme S delle soluzioni della congruenza è costituito da tutti i numeri $x \in \mathbb{Z}$ tali che $[x]=[bc]$ ed è quindi $S=\{bc+nt \mid t \in \mathbb{Z}\}$.

Osservazione 9.7. Se $MCD(a,n)=1$, l'insieme delle soluzioni di $aX \equiv b \bmod n$ è l'insieme $x_0+n\mathbb{Z}=\{x_0+nt \mid t \in \mathbb{Z}\}$, dove x_0 è una qualsiasi soluzione della congruenza. Per determinare tutte le soluzioni è quindi sufficiente conoscerne una qualsiasi.

Osservazione 9.8. Se $MCD(a,n)/b$, la congruenza $aX \equiv b \bmod n$ è risolubile e il suo insieme delle soluzioni si può esprimere mediante una nuova congruenza con coefficiente direttivo 1 ossia del tipo $X \equiv c \bmod m$, dove c è una qualsiasi soluzione della congruenza e $m=n/MCD(a,n)$.

§ 9.3 La funzione di Eulero

Definizione 9.9. *Si chiama* **funzione di Eulero** *l'applicazione* $\phi\colon \mathbb{N}\setminus\{0,1\} \to \mathbb{N}$ *data da* $\phi(n)=Card\{k \in \mathbb{N} \mid 1 \le k < n,\ MCD(n,k)=1\}$*, ossia* $\phi(n)$ *è il numero di interi tra* 1 *e* $n-1$ *coprimi con* n*.*

La funzione di Eulero di un numero n coincide col numero di classi invertibili in $\mathbb{Z}_n$. Ad esempio, se p è un numero primo, $\phi(p)=p-1$, poiché tutte le classi non nulle in $\mathbb{Z}_p$ sono invertibili. Più in generale, se p^k è la potenza di un numero primo $\phi(p^k)=p^{k-1}(p-1)$, poiché in $\mathbb{Z}_{p^k}$ sono invertibili tutte le classi tranne le p^{k-1} classi i cui rappresentanti compresi tra 0 e p^k-1 sono i multipli di p, ossia $p\cdot 0$, $p\cdot 1$, $p\cdot 2$, …, $p\cdot(p^{k-1}-1)$. Vediamo ora un metodo per calcolare il valore di $\phi(n)$ per ogni intero n a partire dalla fattorizzazione di n in fattori primi $p_1^{r_1}\cdots p_k^{r_k}$, con primi p_i tutti distinti.

Proposizione 9.10. (Moltiplicatività della funzione di Eulero) *Siano* $p_1,\dots,p_k$ *primi distinti. Allora :*

$$\phi(p_1^{r_1}\cdots p_k^{r_k})=\phi(p_1^{r_1})\cdots\phi(p_k^{r_k})=p_1^{r_1-1}(p_1-1)\cdots p_k^{r_k-1}(p_k-1).$$

Teorema 9.11. (Teorema di Eulero) *Siano* a,n *interi positivi tali che* $MCD(a,n)=1$*. Allora* $a^{\phi(n)} \equiv 1 \bmod n$*.*

Dimostrazione. La dimostrazione si articola in alcuni punti della cui prova diamo solo una breve traccia. Sia p un numero primo.

I) $(x+y)^p \equiv x^p+y^p \bmod p$. (Il coefficiente binomiale $\binom{p}{k}=\frac{p!}{k!\cdot(p-k)!}$ è multiplo di p per ogni k tale che $1 \le k \le p-1$.)

II) Piccolo teorema di Fermat. $a^p \equiv a \bmod p$. (È sufficiente considerare gli interi $a \geq 0$. Per induzione su a. Se $a = 0$ è ovvio. Se vale per $a-1$, allora $a^p = ((a-1)+1)^p \equiv (a-1)^p + 1^p \equiv (a-1) + 1 = a \bmod p$.)

III) Se p è primo e $MCD(a,p) = 1$, allora $a^{p-1} \equiv 1 \bmod p$. (In $\mathbb{Z}_p$ la classe di a è invertibile e quindi si può cancellare a nella relazione II.)

IV) Si generalizza al caso di un numero $n = p^r$ per induzione su r e la formula dello sviluppo della potenza $p-$esima di un binomio.

V) Si generalizza al caso di un numero qualsiasi usando la decomposizione in potenze di primi. Se $n = p^r t$, con $MCD(p,t) = 1$, allora $a^{\phi(n)} = a^{\phi(p^r)\phi(t)} \equiv 1^{\phi(t)} = 1 \bmod p^r$. Valendo questa relazione rispetto a tutti i primi nella decomposizione di n, allora vale anche modulo n.

□

Esempio 9.12. Consideriamo i due numeri $a = 2$ e $n = 7$ che sono coprimi. Poichè 7 è primo, si ha $\phi(7) = 7 - 1 = 6$. Verifichiamo il Teorema di Eulero in questo caso particolare mediante calcoli diretti:

$$2^6 = 64 = 7 \cdot 9 + 1 \text{ quindi } 64 \equiv 1 \bmod 7 \text{ ossia } 2^{\phi(7)} \equiv 1 \bmod 7.$$

Esempio 9.13. Vogliamo calcolare la cifra x che indica le unità del numero 327^{82} scritta in forma posizionale. Anche un computer incontra grosse difficoltà ad eseguire questo calcolo e in ogni caso fornisce soltanto una approssimazione del risultato data dalle prime cifre a sinistra del numero accompagnate da una opportuna potenza di 10, non certo l'ultima cifra a destra. Eseguiamo in altro modo questo calcolo facendo ricorso al Teorema di Eulero. Osserviamo che calcolare la cifra delle unità equivale a calcolare il resto della divisione per 10 ossia il numero x compreso tra 0 e 9 tale che $\overline{x} = \overline{327^{82}}$ in $\mathbb{Z}_{10}$. Intanto $327 \equiv 7 \bmod 10$ quindi in $\mathbb{Z}_{10}$ si ha $\overline{x} = \overline{327}^{82} = \overline{7}^{82}$. Ora, per il teorema di Eulero con $a = 7$, $n = 10$ e $\phi(n) = \phi(10) = 4$ vale la relazione $7^{\phi(10)} = 7^4 \equiv 1 \bmod 10$. Quindi $\overline{x} = \overline{7}^{82} = \overline{7}^{80+2} = (\overline{7}^4)^{20} \cdot \overline{7^2} = \overline{1}^{20} \cdot \overline{49} = \overline{9}$.
La cifra finale di 327^{82} è quindi 9.

Esempio 9.14. Vogliamo trovare le ultime due cifre decimali (ossia decine e unità) di 3^{925}. Le ultime due cifre decimali corrispondono al resto della divisione per 100. Come nell'esempio precedente usiamo il Teorema di Eulero:

$$a^{\phi(100)} \equiv 1 \bmod 100.$$

Ora $\phi(100) = \phi(25 \cdot 4) = \phi(5^2 \cdot 2^2) = 5(5-1)2(2-1) = 40$ dunque $3^{40} \equiv 1 \bmod 100$. Inoltre $925 = 40 \cdot 23 + 5$ e quindi

$$\overline{3}^{925} = \overline{3}^{23 \cdot 40 + 5} = (\overline{3}^{40})^{23} \cdot \overline{3}^5 = \overline{1} \cdot (\overline{3}^5) = \overline{243} = \overline{43}.$$

Il Teorema di Eulero è alla base di un metodo crittografico particolarmente ingegnoso che risolve il problema della segretezza nello scambio delle "chiavi" tra il mittente e il destinatario.

§ 9.4 Solo per curiosità : Crittografia e RSA

(da *10 lezioni di matematica* di G. Ferrarese, M. Roggero, G. Tamone, Aracne ed.)

La **crittografia**, dal greco $\chi\rho\upsilon\pi\tau o\sigma$ = nascosto e $\gamma\rho\alpha\varphi\epsilon\iota\nu$ = scrivere, è lo studio dei metodi per garantire la segretezza del contenuto di un messaggio anche nel caso sia intercettato. Un metodo crittografico ideale dovrebbe permettere al mittente di crittografare con molta facilità i messaggi e dovrebbe inoltre assicurare che solo il destinatario designato possa decifrarli con facilit'a. Nata come raccolta di tecniche e di sistemi per assicurare la riservatezza di messaggi tra regnanti, imperatori, amanti, etc, la crittografia è maturata definitivamente a rango di scienza solo nei primi del 1900 con l'avvento di nuove teorie e tecniche matematiche. Attualmente è entrata a far parte della nostra vita quotidiana, poiché ne fanno uso tessere Bancomat, telefoni cellulari, trasmissioni televisive, internet e in genere ogni strumento di comunicazione elettronica.
Le sue origini sono antichissime; basti pensare che piú di 6000 anni fa si scrivevano geroglifici egizi in modo non standard e ancora oggi si lavora per la loro interpretazione e che nella Bibbia si trova un esempio di crittografia mediante sostituzione di ogni lettera dell'alfabeto con la lettera che occupa la stessa posizione nell' alfabeto scritto al contrario. I metodi crittografici **a chiave pubblica** non richiedono lo scambio di comunicazioni riservate in alcun momento tra mittente e destinatario. Nel seguito tutte le comunicazioni tra i due soggetti si intenderanno come disponibili a chiunque; ad esempio possono avvenire mediante pubblicazione su un giornale oppure su un sito internet completamente accessibile. La prima metodologia crittografica di questo genere fu sviluppata nel 1978 da tre ricercatori: Ronald Rivest, Adi Shamir e Leonard Adleman; essi realizzarono una procedura che, dalle loro iniziali, prende il nome di "RSA".
L'idea di base del codice RSA è la constatazione , di quanto sia facile moltiplicare tra loro due numeri dati e di quanto sia invece difficile (o meglio calcolativamente lungo) risalire ai fattori dato il prodotto. In teoria chiunque può decifrare un messaggio crittografato mediante il codice RSA, ma il tempo richiesto per la decifrazione è tanto da rendere il messaggio ormai privo di interesse. Il diretto destinatario possiede invece un metodo di decifratura molto veloce. Vediamo come questa "doppia velocità " possa essere praticamente realizzata.
Ci si accorda (pubblicamente!) su come trasformare i messaggi in sequenze di numeri ciascuno di lunghezza prefissata: sia m uno di questi numeri. Il **destinatario** del messaggio prepara la chiave di decifrazione nel modo seguente:

- Costruisce un numero n moltiplicando due numeri primi p e q abbastanza grandi in modo che p e q siano maggiori di m: in questo modo m è sicuramente coprimo con $n = pq$. Inoltre sapendo che $n = pq$ egli può facilmente calcolare la funzione di Eulero $\phi(n) = (p-1)(q-1)$.

- Sceglie inoltre un altro numero h coprimo con $\phi(n)$ e calcola l'inverso $\overline{d}$ di $\overline{h}$ in $\mathbb{Z}_{\phi(n)}$ ossia calcola d tale che $hd = 1 + k\phi(n)$.

- Infine rende pubblici i due numeri n e h, mentre mantiene il piú assoluto segreto sulla fattorizzazione $n = pq$, sul valore di $\phi(n)$ e su d.Il **mittente** adopera queste informazioni, ossia n e h, per crittografare il messaggio m nel modo seguente:

- Calcola la potenza m^h e la divide per n ottenendo un resto c; comunica (pubblicamente) al destinatario il numero c che è il messagio cifrato. La relazione tra il messaggio originale e la sua cifratura è data da:

$$c \equiv m^h \bmod n \quad \text{ovvero} \quad \overline{c} = \overline{m}^h \quad \text{in} \quad \mathbb{Z}_n.$$

- Il destinatario decodifica il messaggio con l'aiuto del numero d calcolando la potenza c^d. Si ha infatti:

$$\overline{c}^d = \overline{m}^{hd} = \overline{m}^{1+k\phi(n)} = \overline{m} \cdot (\overline{m}^k)^{\phi(n)} = \overline{m} \cdot \overline{1} = \overline{m}.$$

  Qualunque sia il numero m' che ottiene come rappresentante della classe $\overline{c}^d = \overline{m}$, egli può infine ricavare m come resto della divisione di m' per n; infatti m (essendo positivo e minore di n) è proprio il resto della divisione per n di ogni numero m' congruo a m modulo n.

Come si può vedere nell'ultimo passaggio la validità del Teorema di Eulero sta alla base di questa procedura. Infatti è grazie a tale risultato che possiamo affermare che $(\overline{m}^k)^{\phi(n)} = \overline{1}$. A titolo di curiosità diciamo che i primi attualmente adoperati per l'RSA hanno un numero di cifre dell'ordine delle centinaia e che il metodo viene considerato del tutto sicuro. In un esperimento del 1994 per rompere una chiave RSA di 129 cifre, (ossia per fattorizzare un numero n di 129 cifre), sono stati necessari 8 mesi di lavoro coordinato effettuato da 600 gruppi di ricerca sparsi in 25 paesi, che hanno messo a disposizione 1600 computers, facendoli lavorare in parallelo collegati tra loro attraverso Internet!

Esempio 9.15. Eseguiamo una simulazione di codifica e decodifica di un messaggio mediante RSA. Il destinatario del messaggio, chiamiamola Francesca, ha scelto i due primi 5 e 11 e li ha moltiplicati ottenendo 55. Perché questa simulazione con numeri cosı piccoli abbia senso dobbiamo fingere che nessuno (a parte Francesca) sia in grado di calcolare in tempi brevi la fattorizzazione di 55. Francesca ha calcolato

$\phi(55) = (5-1)\cdot(11-1) = 40$, ha scelto $h = 3$ coprimo con 40 e ha determinato (mediante l'algoritmo euclideo) un numero d tale che $dh \equiv 1 \bmod 40$, ottenendo $d = 27$ (poiché $3 \cdot 27 = 1 + 2 \cdot 40$). Francesca comunica poi pubblicamente, a tutti coloro che vogliono scriverle in modo riservato, i due numeri $n = 55$ e $h = 3$. Paolo vuole mandarle il messaggio $m = 7$: calcola: $m^h = 7^3 = 343$, lo divide per 55 e ottiene il resto $c = 13$ che spedisce a Francesca. Nessuno è in grado di decodificare il messaggio $c = 13$ tranne Francesca che possiede la chiave di decifrazione $d = 27$. Francesca calcola allora 13^{27} e quindi divide per 55 ottenendo il resto 7 che è il messaggio "in chiaro". Si noti che Francesca non deve necessariamente calcolare per intero la potenza 13^{27} prima di eseguire la divisione per 55, ma può lavorare nelle classi di resto $\mathbb{Z}_{55}$ nel modo seguente:

$$\overline{13}^{27} = (\overline{13}^3)^9 = \overline{52}^9 = \overline{-3}^9 = \overline{-19683} = \overline{-48} = \overline{7}.$$

§ 9.5 Esercizi

9.1 Determinare l'unico numero compreso tra 0 e 52 che stia nella classe di resto modulo 52 di $k = 427$ e poi di $h = -444$.

9.2 Come si fa ad ottenere esattamente 3 litri di acqua usando un recipiente da 5 litri e un altro da 7 litri?

9.3 Eseguire in $\mathbb{Z}_{12}$ i calcoli: $\overline{5}\cdot\overline{3} + \overline{21} - \overline{6}$.

9.4 Scrivere la tabellina del $\overline{5}$ in $\mathbb{Z}_{12}$ ossia: $\overline{5\cdot 0}$, $\overline{5\cdot 1}$, $\overline{5\cdot 2}$ .... Quanto fa $\overline{5\cdot 8734}$?

9.5 Scrivere la lista delle potenze di $\overline{5}$ in $\mathbb{Z}_{12}$ ossia: $\overline{5}^0$, $\overline{5}$, $\overline{5}^2$ .... Quanto fa $\overline{5}^{8734}$?

9.6 Provare che in in $\mathbb{Z}_7$ tutte le classi tranne $\overline{0}$ sono invertibili determinando esplicitamente gli inversi.

9.7 Risolvere le seguenti equazioni in $\mathbb{Z}_7$ mediante sostituzione diretta di ciascun elemento di $\mathbb{Z}_{12}$:

$$\overline{5}x = \overline{1}\ ,\ \overline{2}x = \overline{6}\ ,\ x^2 = \overline{1}\ ,\ x^2 = \overline{0}.$$

9.8 Se $\overline{28} = \overline{2}$ in $\mathbb{Z}_n$, cosa possiamo dire di n?

9.9 Risolvere mediante sostituzione diretta l'equazione in $\mathbb{Z}_8$: $[6]\,[x] = [0]$.

9.10 Calcolare $\phi(100), \phi(528), \phi(121), \phi(297), \phi(700), \phi(215)$

9.11 Trovare la cifra finale di 17^{307} e 18^{75}.

9.12 Calcolare le ultime due cifre di 9^{201} e 302^{46}.

9.13 Fino dalle elementari si imparano alcuni espedienti pratici per riconoscere velocemente se un numero è divisibile per 2, 3, 4, 5 e 11. Ottenere in modo rigoroso questi criteri operando sulle classi di resto in modo analogo a quanto fatto per la prova del 9. Perch non si imparano anche criteri per la divisibilità per 7 o per 13?

9.14 Verificare se la relazione tra i punti del piano per cui due punti sono in relazione se e solo se hanno la stessa distanza dall'origine è una relazione di equivalenza.

9.15 Verificare se la relazione tra le rette del piano per cui due rette sono in relazione se e solo se sono parallele è una relazione di equivalenza.

9.16 Verificare se la relazione tra triangoli del piano per cui due triangoli sono in relazione se e solo se sono simili è una relazione di equivalenza.

9.17 Verificare se la relazione tra le rette del piano per cui due rette sono in relazione se e solo se sono perpendicolari è una relazione di equivalenza.

9.18 Verificare se la relazione tra numeri reali per cui due numeri sono in relazione se e solo se uno dei due divide l'altro è una relazione di equivalenza. **9.19** Sia $X = \mathbb{R}[x]/(x^2+1)$ l'insieme

delle classi di equivalenza di polinomi ottenuto mediante la relazione di equivalenza per cui due polinomi sono equivalenti se e solo se divisi per x^2+1 hanno lo stesso resto. Provare che X è in corrispondenza biunivoca con $\mathbb{C}$.

9.20 Consideriamo $\mathbb{Z}_{54}$, l'anello delle classi di resto modulo 54.

a. Trovare un intero n, $0 \leq n < 54$, tale che $[n] = [125]$. Ne esiste più d'uno?

b. Esiste un intero pari nella classe di 125?

c. Esiste un intero multiplo di 3 nella classe di 125?

d. Sia m un intero fissato. Provare che esiste almeno un intero s, con $100 \leq s \leq 200$, tale che $[m] = [s]$.

9.21 Nell'anello $\mathbb{Z}_{24}$:

a. determinare tutti gli elementi invertibili e le loro classi;

b. determinare tutti gli zero-divisori;

c. trovare tutti gli elementi $[b]$ tali che $[b] \cdot [16] = [0]$.

d. Provare che $[5^k]$ è invertibile in $\mathbb{Z}_{24}$ per ogni $k \in \mathbb{N}$. Possiamo allora dire che gli elementi invertibili di $\mathbb{Z}_{24}$ sono infiniti?

9.22 Si determini (se esiste) l'inverso di $[2]^{1432}$ in $\mathbb{Z}_{29}$.

9.23 L'equazione $[3522] \cdot [x] = [1]$ ha soluzioni in $\mathbb{Z}_{500}$?

9.24 Risolvere le congruenze:

$$3x \equiv 7 \bmod 11 \qquad 8x \equiv 18 \bmod 30 \qquad 9x \equiv 12 \bmod 20$$

$$2x \equiv 11 \bmod 13 \qquad 8x \equiv 4 \bmod 10 \qquad 4x \equiv 7 \bmod 15$$

9.25 Calcolare $\phi(36)$, $\phi(528)$ e $\phi(121)$, dove ϕ è la funzione di Eulero.

9.26 Determinare la cifra delle unità del numero 3477^{159}.

9.27 Determinare la cifra delle unità e quella delle centinaia del numero 17^{1609}.

9.28 Risolvere la congruenza $2x \equiv 10^{712} \mod 11$.

9.29 Determinare il generatore del sottogruppo $H =< 36, 30 >$ di $(\mathbb{Z}, +)$.

9.30 Nel gruppo $(\mathbb{Z}_{55}, +)$ delle classi di resto modulo 55:

(a) Determinare il numero di elementi del sottogruppo ciclico di generato da $[10]_{55}$.

(b) Verificare che il sottogruppo ciclico generato da $[12]_{55}$ coincide con tutto $\mathbb{Z}_{55}$.

(c) Scrivere tutti gli elementi del sottogruppo ciclico generato da $[10]_{55}$.

(d) Dimostrare che $(\mathbb{Z}_{55} - \{0\}, \cdot)$ non à un gruppo.

9.31 Determinare tutti gli elementi del gruppo $(\mathbb{Z}_{16}^*, \cdot)$ e il periodo di ciascuno. Dedurre da quanto ottenuto se $(\mathbb{Z}_{16}^*, \cdot)$ à un gruppo ciclico?

9.32 Determinare tutti gli elementi del gruppo $(\mathbb{Z}_{12}^*, \cdot)$ e il periodo di ciascuno. Dedurre da quanto ottenuto se $(\mathbb{Z}_{12}^*, \cdot)$ à un gruppo ciclico?