LICEO *B. RUSSELL* – A.S. 2010/2011 –

DALLA TEORIA DEI NUMERI ALLE CONGRUENZE

Tutti i numeri qui considerati sono interi. Se si tratta in particolare di numeri Naturali (quindi non negativi) verrà specificato.

1. Divisibiltà

Dati due numeri (interi) a e b diciamo che a divide b, in simboli $a|b$, se esiste un numero (intero) c tale che $b = a \cdot c$.

$$a|b \qquad \text{se } b = a \cdot c$$

Esempio.

$$4|12 \qquad \text{perché } \ 12 = 4 \cdot 3$$

Osservazioni.

- Tutti i numeri a dividono le zero in quanto $0 = a \cdot 0$ per ogni a. In particolare anche 0 divide se stesso.
- Vale la proprietà transitiva:

Proprietà 1. *Se $a|b$ e $b|c$ allora $a|c$.*

Per esempio $2|4$ e $4|12$ implica che $2|12$.

Dimostrazione. Se $a|b$ e $b|c$ si ha $b = na$ e $c = mb$ per qualche $n, m \in \mathbb{Z}$. Di conseguenza $c = m(na) = (mn)a$ dove $mn \in \mathbb{Z}$ e quindi $a|c$.

□

Vale inoltre la seguente importante proprietà.

Proprietà 2. *Se $a = b + c$ e d divide due dei tre numeri a, b e c, allora divide anche il terzo.*

Dimostrazione. Supponiamo per esempio che d divida b e c, cioè esistono $n, m \in \mathbb{Z}$ tali che $b = nd$ e $c = md$. Di conseguenza

$$a = b + c = nd + md = (m + n)d$$

Poiché $n + m \in \mathbb{Z}$, questo equivale a dire che d divide a.

Analogamente si procede per dimostrare gli altri casi.

□

Tra i numeri naturali hanno un ruolo fondamentale i numeri primi: un numero naturale diverso da 1 è detto **primo** se è solo divisibile per se stesso e per 1, cioè se ammette solo i due divisori banali.

In $\mathbb{N}$ vale il seguente

Teorema 1. Teorema fondamentale dell'algebra. *Ogni numero naturale può essere scritto in maniera unica (a meno dell'ordine) come prodotto di potenze di numeri primi:*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

La scomposizione in fattori primi di un numero n ci fornisce molte informazioni sul numero:

- Tutti i divisori di n sono dati dalle possibili combinazioni dei primi p_i, elevati a potenze non superiori a α_i. Per esempio: $12 = 2^2 \cdot 3$ e i divisori di 12 sono

  $$1, \quad 3, \qquad 2, \quad 2 \cdot 3, \qquad 2^2, \quad 2^2 \cdot 3$$

  Otteniamo quindi $2 \cdot 3 = 6$ possibili divisori, dati dalle due potenze di 3 possibili ($3^0 = 1,\ 3^1$) combinate con le tre potenze di 2 possibili ($2^0 = 1,\ 2^1,\ 2^2$).

  In generale un numero naturale

  $$\boxed{n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k} \text{ ha esattamente } (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1) \text{ divisori distinti.}}$$

- Tutti i multipli di n devono contenere tra i loro fattori tutti i fattori primi p_i, elevati almeno alla potenza α_i.

Un'altra proprietà molto utile dei numeri primi è la seguente

Date: December 6, 2010.

Proprietà 3. *Se un numero primo p divide il prodotto di due numeri interi a e b, allora p divide uno dei due fattori:*

$$p|ab \quad \Rightarrow \; p|a \vee p|b.$$

Per esempio $3|48 = 12\cdot 4$ e infatti $3|12$. Questo non avviene per i numeri non primi; per esempio $4|12 = 2\cdot 6$, ma 4 non divide nè 2 nè 6. Questa proprietà è utilizzata per dimostrare che $\sqrt{2}$ è irrazionale.

2. MCD e mcm tra numeri

Conosciamo le seguenti definizioni di MCD e di mcm tra due numeri Naturali a e b (non sono le migliori definizioni, ma vanno bene per quello che dobbiamo fare):

- *Il Massimo Comune Divisore tra due numeri Naturali a e b il più grande tra i numeri naturali che dividono sia a che b*

  Esempio. $\mathrm{MCD}(18, 12) = 6$
- *Il minimo comune multiplo tra due numeri Naturali a e b il più piccolo tra i numeri naturali che sono multipli sia di a che di b*

  Esempio. $\mathrm{mcm}(18, 12) = 36$

A parte i casi banali come quello precedente, sappiamo calcolare il Massimo Comune Divisore e il minimo comune multiplo di due numeri scomponendoli in fattori:

Esempio. Siano $n = 2^4 \cdot 3^5 \cdot 7$ e $m = 2^3 \cdot 7^2 \cdot 11^4$. Allora

$$\mathrm{MCD}(n, m) = 2^3 \cdot 7 \qquad \mathrm{mcm}(n, m) = 2^4 \cdot 3^5 \cdot 7^2 \cdot 11^4$$

Come osservato precedentemente, non è però sempre semplice scomporre un numero in fattori primi. In tali casi si può lavorare in maniera completamente diversa.

Ricordiamo il seguente importante toerema

Teorema 2. Divisione con resto *Dati due numeri a e b, esistono unici q e r tali che*

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

Il numero q è detto quoziente e r resto della divisione tra a e b.

Esempio. Eseguendo la divisione tra 11 e 4 otteniamo quoziente 2 e resto 3, quindi

$$11 = 4 \cdot 2 + 3$$

In particolare se $r = 0$, allora $a = bq$, ovvero $b|a$.

Come diretta conseguenza della **Proprietà 2**, abbiamo che se $a = bq + r$, allora

$$d|a \text{ e } d|b \;\Leftrightarrow\; d|b \text{ e } d|r$$

Di conseguenza i divisori comuni ad a e b sono i divisori comuni a b e r e quindi $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, r)$.

Iterando il processo della divisione con resto si può calcolare il MCD tra coppie di numeri successivamente più piccole, fino ad arrivare alla situazione banale.

Esempio. Cerchiamo il $\mathrm{MCD}(18, 12)$. Eseguiamo la divisione tra 18 e 12:

$$18 = 12 \cdot 1 + 6 \qquad \text{e} \qquad \mathrm{MCD}(18, 12) = \mathrm{MCD}(12, 6)$$

Ora eseguiamo la divisione tra 12 e 6, il resto appena determinato:

$$12 = 6 \cdot 2 + 0 \qquad \text{quindi} \qquad \mathrm{MCD}(12, 6) = 6$$

L'ultimo resto non nullo è il MCD cercato: $\mathrm{MCD}(18, 12) = 6$. Infatti dal momento che 6 divide 12, $\mathrm{MCD}(12, 6) = 6$ (la situazione banale verso cui puntavamo).

Esempio. Cerchiamo il $\mathrm{MCD}(30, 8)$. Eseguiamo la divisione tra 30 e 8:

$$30 = 8 \cdot 3 + 6 \qquad \text{e} \qquad \mathrm{MCD}(30, 8) = \mathrm{MCD}(8, 6)$$

Ora eseguiamo la divisione tra 8 e 6, il resto appena determinato:

$$8 = 6 \cdot 1 + 2 \qquad \text{e} \qquad \text{MCD}(8,6) = \text{MCD}(6,2)$$

Ora eseguiamo la divisione tra 6 e 2, il resto appena determinato:

$$6 = 2 \cdot 3 + 0 \qquad \text{quindi} \qquad \text{MCD}(6,2) = 2$$

L'ultimo resto non nullo è il MCD cercato: $\text{MCD}(30,8) = 2$

Esempio. Cerchiamo il $\text{MCD}(124,34)$. Eseguiamo la divisione tra 124 e 36:

$$124 = 36 \cdot 3 + 22 \qquad \text{e} \qquad \text{MCD}(124,36) = \text{MCD}(36,22)$$

Ora eseguiamo la divisione tra 36 e 22, il resto appena determinato:

$$36 = 22 \cdot 1 + 14 \qquad \text{e} \qquad \text{MCD}(36,22) = \text{MCD}(22,14)$$

Ora eseguiamo la divisione tra 22 e 14, il resto appena determinato:

$$22 = 14 \cdot 1 + 8 \qquad \text{e} \qquad \text{MCD}(22,14) = \text{MCD}(14,8)$$

Ora eseguiamo la divisione tra 14 e 8, il resto appena determinato:

$$14 = 8 \cdot 1 + 6 \qquad \text{e} \qquad \text{MCD}(14,8) = \text{MCD}(8,6)$$

Ora eseguiamo la divisione tra 8 e 6, il resto appena determinato:

$$8 = 6 \cdot 1 + 2 \qquad \text{e} \qquad \text{MCD}(8,6) = \text{MCD}(6,2)$$

Ora eseguiamo la divisione tra 6 e 2, il resto appena determinato:

$$6 = 2 \cdot 3 + 0 \qquad \text{quindi} \qquad \text{MCD}(6,2) = 2$$

L'ultimo resto non nullo è il MCD cercato: $\text{MCD}(124,34) = 2$. Naturalmente ci si può fermare nel processo in ogni punto ritenuto ragionevole. In realtà per numeri piccoli come quelli degli esempi può essere più veloce il vecchio metodo, ma per numeri grandi l'algoritmo di Euclide risulta molto più veloce.

Esempio. Calcoliamo il $\text{MCD}(5812079, 11501)$.

$$\begin{aligned}
5812079 &= 11501 \cdot 505 + 4074 \\
11501 &= 4074 \cdot 2 + 3353 \\
4074 &= 3353 \cdot 1 + 721 \\
3353 &= 721 \cdot 4 + 469 \\
721 &= 469 \cdot 1 + 252 \\
469 &= 252 \cdot 1 + 217 \\
252 &= 217 \cdot 1 + 35 \\
217 &= 35 \cdot 6 + 7 \\
35 &= 7 \cdot 5 + 0
\end{aligned}$$

Quindi $\text{MCD}(5812079, 11501) = 7$

Tale metodo ha inoltre utilità in applicazione del seguente teorema.

Teorema 3. *Sia $d = MCD(a,b)$. Allora esistono due numeri x, y tali che*

$$d = ax + by$$

Per trovare tali x, y è sufficiente ripercorrere a ritroso l'algoritmo della divisione.

Esempio. Abbiamo calcolato prima il $\text{MCD}(30,8)$:

$$\begin{aligned}
30 &= 8 \cdot 3 + 6 \\
8 &= 6 \cdot 1 + 2 \\
6 &= 2 \cdot 3 + 0
\end{aligned}$$

Oserviamo ora che

$$\begin{aligned}
30 &= 8 \cdot 3 + 6 && \Rightarrow 6 = 30 - 8 \cdot 3 \\
8 &= 6 \cdot 1 + 2 && \Rightarrow 2 = 8 - 6 \cdot 1 \\
6 &= 2 \cdot 3 + 0
\end{aligned}$$

Sostituiamo ora 6, ricavato dalla prima equazione, nella seconda, ottenendo

$$2 = 8 - 6 \cdot 1 = 8 - (30 - 8) \cdot 1 = 8 - 30 + 8 = -30 + 2 \cdot 8$$

Quindi

$$2 = -1 \cdot 30 + 2 \cdot 8$$

E i numeri cercati sono $x = -1$ e $y = 2$.

Esempio. Calcoliamo il MCD$(83, 58)$:

$$\begin{aligned} 83 &= 58 \cdot 1 + 25 \\ 58 &= 25 \cdot 2 + 8 \\ 25 &= 8 \cdot 3 + 1 \\ 8 &= 1 \cdot 8 + 0 \end{aligned}$$

Quindi MCD$(83, 58) = 1$. In questi casi in cui MCD=1, diciamo che 83 e 58 sono **coprimi**. Osserviamo ora che

$$\begin{aligned} 83 &= 58 \cdot 1 + 25 && \Rightarrow 25 = 83 - 58 \\ 58 &= 25 \cdot 2 + 8 && \Rightarrow 8 = 58 - 25 \cdot 2 \\ 25 &= 8 \cdot 3 + 1 && \Rightarrow 1 = 25 - 8 \cdot 3 \end{aligned}$$

Sostituiamo ora i valori ricavati cominciando dal fondo

$$\begin{aligned} 1 &= 25 - 8 \cdot 3 \\ &= 25 - (58 - 25 \cdot 2) \cdot 3 = 58 \cdot (-3) + 25 \cdot 7 \\ &= 58 \cdot (-3) + (83 - 58) \cdot 7 = 83 \cdot 7 + 58 \cdot (-10) \end{aligned}$$

Quindi

$$1 = 83 \cdot 7 + 58 \cdot (-10)$$

E i numeri cercati sono $x = 7$ e $y = -10$.

Un'importante conseguenza di questo teorema è dato dalla seguente proprietà

Proprietà 4. *Dati $a, b \in \mathbb{Z}$, esistono $r, s \in \mathbb{Z}$ tali che $ra + sb = 1$ se e solo se $MCD(a, b) = 1$.*

Dimostrazione.

□

Fino ad ora ci siamo in sostanza occupati del Massimo Comune Denominatore; in realtà, noto questo, possiamo immediatamente ricavare il minimo comune multiplo.

Proprietà 5. *Dati due numeri a e b vale la seguente relazione:*

$$mcm(a, b) = \frac{a \cdot b}{MCD(a, b)}$$

3. Congruenze-algebra modulare

Sia $n \in \mathbb{N}$ fissato e siano $a, b \in \mathbb{Z}$, diciamo che a è congruo a b modulo n, in simboli

$$a \equiv b \pmod{n}$$

se a e b divisi per n hanno lo stesso resto.

Esempio.

$$8 \equiv 17 \pmod{3} \equiv 2 \pmod{3}$$

perché

$$\begin{aligned} 8 &= 2 \cdot 3 + 2 \\ 17 &= 5 \cdot 3 + 2 \\ 2 &= 0 \cdot 3 + 2 \end{aligned}$$

Definiamo quindi la **classe di equivalenza** di a modulo n l'insieme di tutti i numeri che hanno lo stesso resto di a nella divisione per n. Indichiamo tale insieme con $[a]_n$, anche detto **classe di congruenza** o **classe di resto** di a modulo n:

$$[a]_n = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$$

Esempio.

$$[2]_3 = \{\dots 2, 5, 8, 11, 14, \dots, 332, \dots\}$$

I puntini che precedono il 2 indicano che in $[2]_3$ sono presenti anche numeri negativi. Per trovare tali numeri piuttosto che fare la divisione con resto (inusuale tra numeri negativi) è più comodo usare la seguente proprietà.

Proprietà 6. *La definizione di congruenza è equivalente a*

$$a \equiv b \pmod{n}$$

se $n|a-b$ (cioè se n divide $a-b$). Notiamo che questo equivale a dire che $a-b=kn$, ovvero che $a=b+kn$ per qualche $k \in \mathbb{Z}$.

Esempio. Abbiamo osservato prima che

$$8 \equiv 17 \pmod{3} \equiv 2 \pmod{3}$$

In effetti

$$3|17-8=9 \qquad \text{e} \quad 3|8-2=6 \qquad \text{e} \quad 3|17-2=15$$

Esempio.

$$-1 \equiv 2 \pmod{3} \text{ perché } 3|-1-2=-3, \text{ oppure perché } -1=2-3$$
$$-4 \equiv 2 \pmod{3} \text{ perché } 3|-4-2=-6, \text{ oppure perché } -4=2-2\cdot 3$$

Vale anche la seguente proprietà, diretta conseguenza della transitività dell'uguale:

Proprietà Se $a \equiv b \pmod{n}$ allora $[a]_n = [b]_n$

Esempio. Dato che $3 \equiv 8 \pmod{5}$, allora $[3]_5 = [8]_5$.

Tra le infinite scelte possibili per rappresentare una classe di equivalenza modulo n in genere si sceglie il numero positivo più piccolo, che sarà quindi un numero minore di n.

Esempio. Le classi di equivalenza modulo 5 sono:

$$[0]_5,\ [1]_5,\ [2]_5,\ [3]_5,\ [4]_5$$

4. Operazioni con le congruenze

Con le classi di congruenza si possono eseguire tutte le operazioni interne all'insieme $\mathbb{Z}$.

- ADDIZIONE.

  $$[a]_n + [b]_n = [a+b]_n$$

  Esempio. Consideriamo le classi di congruenza modulo 10, e consideriamo $a=6$ e $b=7$, quindi $6+7=13$. Tra classi:

  $$[6]_{10} + [7]_{10} = [13]_{10} = [3]_{10}$$

- MOLTIPLICAZIONE.

  $$[a]_n \cdot [b]_n = [a \cdot b]_n$$

  Esempio. Consideriamo le classi di congruenza modulo 10, e consideriamo $a=6$ e $b=7$, quindi $6 \cdot 7 = 42$. Tra classi:

  $$[6]_{10} \cdot [7]_{10} = [42]_{10} = [2]_{10}$$

- SOTTRAZIONE.

$$[a]_n - [b]_n = [a-b]_n$$

ESEMPIO. Consideriamo le classi di congruenza modulo 10, e consideriamo $a = 6$ e $b = 7$, quindi $6 - 7 = -1$. Tra classi:

$$[6]_{10} - [7]_{10} = [-1]_{10} = [9]_{10}$$

- ELEVAMENTO a QUADRATO (e a una qualsiasi potenza in generale).

$$[a]_n^2 = [a^2]_n$$

ESEMPIO. Consideriamo le classi di congruenza modulo 10, e consideriamo $a = 8$. Tra classi:

$$[8]_{10}^2 = [8^2]_{10} = [64]_{10} = [4]_{10}$$

Notiamo che

$$[8]_{10}^2 = [-2]_{10}^2 = [(-2)^2]_{10} = [4]_{10}$$

Notiamo che non è in generale eseguibile la divisione, ma bisogna a ricorrere alla definizione di operazione inversa del prodotto. In generale è quindi bene evitare tale operazione. Per esempio lavorando nelle classi di resto modulo 10 non ha senso l'operazione di divisione per 2 in quanto il risultato non è univocamente determinato. Per esempio volendo eseguire $[16]_{10} : [2]_{10}$ si potrebbe pensare che il risultato è $[8]_{10}$. D'altra parte però $[16]_{10} = [6]_{10}$, quindi $[16]_{10} : [2]_{10} = [6]_{10} : [2]_{10}$ e in questo caso si potrebbe pensare che il risultato è $[3]_{10}$. Questo è dovuto al fatto che esistono più elementi che moltiplicati per $[2]_{10}$ danno come risultato $[6]_{10}$ e più in generale al fatto che $[2]_{10}$ non è un elemento invertibile: non esiste alcun elemento $[a]_{10}$ tale che $[a]_{10} \cdot [2]_{10} = [1]_{10}$; come accennato sopra, la divisione è definita come operazione inversa del prodotto e il fatto che non esista l'inverso di un elemento, implica che la divisione per quell'elemento non sia ben definita.

Enunciamo la seguente proprietà utile per capire quando un elemento è invertibile, ovvero quando si può eseguire tranquillamente la divisione per tale elemento.

Proprietà 7. *Un elemento $[a]_n$ è invertibile se esiste un $[b]_n$ tale che $[a \cdot b]_n = [1]_n$, ovvero se $MCD(a, n) = 1$.*

Sulle operazioni tra classi di congruenza si basano i criteri di divisibilità tra numeri. Ad esempio tutti sappiamo che un numero n è divisibile per 3 se è divisibile per 3 il numero ottenuto sommando le cifre del numero iniziale n. Dal punto di vista delle classi di congruenza, un numero n è divisibile per 3 se $[n]_3 = [0]_3$ (il che significa appunto che il resto della divisione di n per 3 è 0). Ora, supponiamo n di quattro cifre: $n = a_3 10^3 + a_2 10^2 + a_1 10 + a_0$, quindi

$$[n]_3 = \left[a_3 10^3 + a_2 10^2 + a_1 10 + a_0\right]_3 = [a_3]_3[10^3]_3 + [a_2]_3[10^2]_3 + [a_1]_3[10]_3 + [a_0]_3$$

D'altra parte, $[10]_3 = [1]_3$, quindi $[10^2]_3 = [10^3]_3 = [1]_3$. Sostituendo nella precedente uguaglianza:

$$\begin{aligned}[n]_3 &= [a_3]_3[10^3]_3 + [a_2]_3[10^2]_3 + [a_1]_3[10]_3 + [a_0]_3 = [a_3]_3[1]_3 + [a_2]_3[1]_3 + [a_1]_3[1]_3 + [a_0]_3 \\ &= [a_3 + a_2 + a_1 + a_0]_3\end{aligned}$$

cioè proprio il noto criterio.

In maniera del tutto analoga si potrebbe ricavare il criterio di congruenza per un qualsiasi primo p (ma non sempre si ottiene una cosa così comoda da essere degne di essere ricordata). Ad esempio proviamo a ricavare un criterio di divisibilità per 11: supponiamo n di cinque cifre: $n = a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10 + a_0$, quindi

$$\begin{aligned}[n]_{11} &= \left[a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10 + a_0\right]_{11} \\ &= [a_4]_{11}[10^4]_{11} + [a_3]_{11}[10^3]_{11} + [a_2]_{11}[10^2]_{11} + [a_1]_{11}[10]_{11} + [a_0]_{11}\end{aligned}$$

D'altra parte, $[10]_{11} = [-1]_{11}$, quindi $[10^2]_{11} = [10^4]_{11} = [1]_{11}$, mentre $[10]_{11} = [10^3]_{11} = [-1]_{11}$. Sostituendo nella precedente uguaglianza:

$$\begin{aligned}[n]_{11} &= [a_4]_{11}[10^4]_{11} + [a_3]_{11}[10^3]_{11} + [a_2]_{11}[10^2]_{11} + [a_1]_{11}[10]_{11} + [a_0]_{11} \\ &= [a_4]_{11}[1]_{11} + [a_3]_{11}[-1]_{11} + [a_2]_{11}[1]_{11} + [a_1]_{11}[-1]_{11} + [a_0]_{11} \\ &= [a_4 - a_3 + a_2 - a_1 + a_0]_3\end{aligned}$$

Quindi un numero n è divisibile per 11 se è divisibile per 11 il numero ottenuto sommando le cifre di posizione pari e sottraendo le cifre di posizione dispari (partendo dalla cifra delle unità di posizione pari 0).

Esercizio 1. *Utilizzando le classi di congruenza (modulo 10) dimostrare che il numero 3.751.233 non è un quadrato. Quale può essere l'ultima cifra di un numero affinchè questo abbia la speranza di essere un quadrato? (Notiamo che se $x = y^2$, allora anche $[x]_{10} = [y^2]_{10}$)*

Esercizio 2. *Nellle classi di congruenza modulo* 10 *è possibile esguire la divisione* [1] *diviso* [3]*? (Si tratta di vedere se esiste un numero* x *tale che* $[x] \cdot [3] = [1]$*).*

Esercizio 3. *Dimostrare con un esempio che nelle classi di congruenza modulo* 6 *non vale più la legge di annullamento del prodotto, cioè che*

$$[a]_6 \cdot [b]_6 = [0]_6 \quad \not\Rightarrow \quad [a]_6 = [0]_6 \text{ oppure } [b]_6 = [0]_6$$

Provare a generalizzare le classi in cui tale legge non vale.

5. I numeri primi

Consideriamo in questa sezione i numeri primi dispari (cioè diversi da 2). I numeri primi p hanno notevoli proprietà all'interno delle classi di equivalenza. Tra queste ricordiamo il

Teorema 4 (Eulero-Fermat)**.** *Se* $a \not\equiv 0 \pmod p$*, allora*

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

Esempio. Verifichiamo il teorema modulo 5. Notiamo che è sufficiente calcolare le potenze per $1 \leq a \leq 4$, in quanto, per esempio

$$7^4 \equiv 2^4 \pmod 5 \text{ dato che } [7]_5 = [2]_5$$

In questo caso $p - 1 = 4$.

$$\begin{aligned} 1^4 = 1 &\equiv 1 \pmod 5 \\ 2^4 = 16 &\equiv 1 \pmod 5 \\ 3^4 = 81 &\equiv 1 \pmod 5 \\ 4^4 = 256 &\equiv 1 \pmod 5 \end{aligned}$$

Notiamo anche che per semplificare i conti potevamo calcolare

$$\begin{aligned} 3^4 \equiv (-2)^4 = 2^4 = 16 &\equiv 1 \pmod 5 \\ 4^4 \equiv (-1)^4 = 1 &\pmod 5 \end{aligned}$$

6. Quadrati e numeri primi

Consideriamo le classi di congruenza modulo 7 e calcoliamo i quadrati delle possibili classi:

classe	conti	quadrato
$[0]$	$[0]^2 = [0]$	$[0]$
$[1]$	$[1]^2 = [1]$	$[1]$
$[2]$	$[2]^2 = [4]$	$[4]$
$[3]$	$[3]^2 = [9] = [2]$	$[2]$
$[4]$	$[4]^2 = [-3]^2 = [2]$	$[2]$
$[5]$	$[5]^2 = [-1]^2 = [4]$	$[4]$
$[6]$	$[6]^2 = [-1]^2 = [1]$	$[1]$

Quindi nelle classi di congruenza modulo 7 posso, in un certo senso calcolare $\sqrt{2}$, nel senso che si può trovare un numero (in realtà due numeri) che sono soluzione dell'equazione

$$x^2 \equiv 2 \pmod 7 \text{ ovvero } [x]_7^2 = [2]_7$$

Tali numeri sono 3 e 4 ovvero $[3]_7$ e $[4]_7 = [-3]_7$

Osservazioni. Chiaramente tutti i numeri che sono quadrati in $\mathbb{Z}$, restano quadrati nelle classi di congruenza modulo n. In generale però nelle classi di congruenza modulo n ci sono molti più quadrati che in $\mathbb{Z}$.

Esercizio 4. *Determinare tutti i possibili quadrati nelle classi di congruenza modulo* 6 *e* 11*, in maniera analoga a quanto fatto nelle classi di congruenza modulo* 7*.*

Già in $\mathbb{Z}$ non è facile calcolare le radici quadrate di un numero (se non conoscendo i possibili quadrati). Altrettanto difficile è la cosa nelle classi di congruenza. Anche in questo caso ci vengono in aiuto i numeri primi.

Consideriamo i numeri primi p dispari (cioè diversi da 2). Allora $p-1$ è pari e $\frac{p-1}{2}$ è un intero. Vale la seguente proprietà:

Proprietà 8. *a è un quadrato modulo p se e solo se:*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Dimostrazione. Dimostriamo solo l'implicazione diretta. Supponiamo che a sia un quadrato modulo p, allora $a \equiv x^2 \pmod p$ per qualche x. Quindi:

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$$

dove l'ultima uguaglianza deriva dal Teorema di Eulero-Fermat.

□

Vale inoltre la seguente proprietà:

Proprietà 9. *a non è un quadrato modulo p allora*

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

Inoltre

Proprietà 10. *Nelle classi di congruenza modulo p esistono esattamente $\dfrac{p-1}{2}$ elementi a tali che $1 \leq a \leq p-1$ che sono quadrati e altrettanti che non sono quadrati*

In sostanza, se escludiamo i numeri congrui a zero modulo p, tra gli altri esattamente metà sono quadrati. Notiamo inoltre che anche i numeri congrui a zero modulo p sono quadrati in quanto se $a \equiv 0 \pmod p$, allora

$$a \equiv 0^2 \pmod p$$