MARTEDÌ 16-18 LEZ. RECUPERO

TEOREMA CINESE DEL RESTO (CRT)

$$\begin{cases} X \equiv a_1 \pmod{m_1} \\ X \equiv a_2 \pmod{m_2} \end{cases}$$

se m_1 e m_2 primi tra loro, esiste una e una sola soluzione mod $m_1 m_2$

$$\begin{cases} x \equiv 2 \ (7) \\ x \equiv 0 \ (3) \end{cases} \quad \exists! \ a \in \mathbb{Z}/(21) \text{ t.c. } x \equiv a \ (21)$$

$$\mathbb{Z}/(3) \times \mathbb{Z}/(7) \overset{1:1}{\longleftrightarrow} \mathbb{Z}/(21)$$

	0	1	2	3	4	5	6
0	0	15	9	3	18	12	6
1	7	1	16	10	4	19	13
2	14	8	2	17	11	5	20

$$\begin{cases} x \equiv 5 \ (7) \\ x \equiv 1 \ (3) \end{cases} \quad 19$$

Es Trovare le soluzioni intere di

(i) $4x \equiv 11 \pmod{21}$

(ii) $x^2 \equiv 1 \pmod{15}$

→ non primi tra loro

(i) $4x \equiv 11 \pmod{21}$ moltiplico per 4^{-1} $4x \equiv 1 \pmod{21}$

$4x + 21y = 11$

$4a + 21b = 1$

A occhio!

$b = 1 \quad 21$

$21 - 4 \cdot 5 = 1$

$4 \cdot (-5) \equiv 1 \pmod{21}$

$-5 \cdot 4x \equiv 11 \cdot (-5) \pmod{21}$

$\Downarrow$

$x \equiv -55 \equiv -13 \equiv 8 \pmod{21}$

ii) $X^2 \equiv 1 \quad (15)$

modo 1:

provo tutti gli elementi di $\mathbb{Z}/15\mathbb{Z}$

$0^2 \equiv 0$

$1^2 \equiv 1$

$2^2 \equiv 4$

$3^2 \equiv 9$

$4^2 \equiv 16 \equiv 1$

$5^2 \equiv 25 \equiv 10$

$6^2 \equiv 36 \equiv 6$

$7^2 \equiv 49 \equiv 4$

$14^2 \equiv 1$

$13^2 \equiv 4$

$12^2 \equiv 9$

$11^2 \equiv 1$

$10^2 \equiv (-5)^2 \equiv 10$

$9^2 \equiv (-6)^2 \equiv 6^2 \equiv 6$

$8^2 \equiv (-7)^2 \equiv (-1)^2(7^2) \equiv 7^2 \equiv 4$

$1, 4, 11, 14$

Modo 2 (per risolvere ii: $x^2 \equiv 1 \ (15)$)

$$\Updownarrow$$

$$15 \mid x^2-1=(x+1)(x-1)$$

$(x+1)(x-1)$ dev'essere multiplo di 15, cioè di 3 e di 5

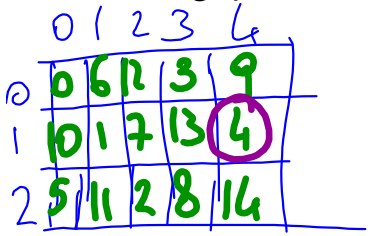
Per il 3, due possibilità: $3 \mid x+1 \iff x \equiv -1 \ (3)$

$3 \mid x-1 \iff x \equiv 1 \ (3)$

Per il 5, $5 \mid x+1 \iff x \equiv -1 \ (5)$

$5 \mid x-1 \iff x \equiv 1 \ (5)$

4 casi: $3 \cdot 5 \mid (x+1)(x-1)$



3 o sta qui o lì

5 o sta qui o lì

L'equazione $x^2 \equiv 1 \ (15)$

equivale a uno di questi 4 casi:

i) $\begin{cases} x \equiv 1 \ (3) \\ x \equiv 1 \ (5) \end{cases} \iff x \equiv 1 \ (15)$

ii) $\begin{cases} x \equiv -1 \ (3) \\ x \equiv -1 \ (5) \end{cases} \iff x \equiv 14 \ (15)$

iii) $\begin{cases} x \equiv 1 \ (3) \\ x \equiv -1 \ (5) \end{cases} \iff x \equiv 4 \ (15)$

iv) $\begin{cases} x \equiv -1 \ (3) \\ x \equiv 1 \ (5) \end{cases} \iff x \equiv 11 \ (15)$

Sol di $x^2 \equiv 1 \ (15)$ = Unione delle sol. nei 4 casi

Parentesi: cosa succede alla tabella se i moduli non sono primi tra loro? 4, 6

2·4

	0	1	2	3	4	5
0	0; 12		8 20		4 16	
1		1; 13		9 21		5 17
2	6 18		2; 14		10 22	
3		7 19		3 15		11 23

$24k+12$

non ci sono #

$\begin{cases} x \equiv 0 \ (4) & \text{pari} \\ x \equiv 1 \ (6) & \text{disp.} \end{cases}$

$$(S)\begin{cases} 4x \equiv 11 \ (21) \\ x^2 \equiv 1 \ (15) \end{cases} \longleftrightarrow \begin{array}{l} x \equiv 8 \ (21) \\ x \equiv 1, 4, 11 \text{ oppure } 14 \ (15) \end{array}$$

Le soluzioni di (S) si ottengono prendendo

$$\begin{cases} x \equiv 8 \ (21) \\ x \equiv 1 \ (15) \end{cases} \quad \begin{cases} x \equiv 8 \ (21) \\ x \equiv 4 \ (15) \end{cases} \quad \begin{cases} x \equiv 8 \ (21) \\ x \equiv 11 \ (15) \end{cases} \quad \begin{cases} x \equiv 8 \ (21) \\ x \equiv 14 \ (15) \end{cases}$$

(1) (2) (3) (4)

no sol no sol. 71 mod 105 29 mod 105

Partiamo dalla (3)

$$\begin{cases} x \equiv 8 \pmod{21} \\ x \equiv 11 \pmod{15} \end{cases}$$

$x \equiv 8 \equiv 1 \pmod 7$

$x \equiv 8 \equiv 2 \pmod 3$

$x \equiv 11 \equiv 1 \pmod 5$

$x \equiv 11 \equiv 2 \pmod 3$

$$\Leftrightarrow \begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 3 \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 5 \end{cases}$$

$$\Leftrightarrow \begin{cases} x \equiv 1 \pmod{35} \\ x \equiv 2 \pmod 3 \end{cases} \Leftrightarrow \begin{cases} x \equiv 71 \pmod{105} \end{cases}$$

$35 \cdot 3 = 105$

$$\begin{array}{r} 1 \\ 36 \\ 71 \end{array}$$

1) $\begin{cases} x \equiv 8 \pmod{21} \\ x \equiv 1 \pmod{15} \end{cases}$

$x \equiv 8 \pmod{21}$ → $x \equiv 1 \pmod 7$, $x \equiv 2 \pmod 3$

$x \equiv 1 \pmod{15}$ → $x \equiv 1 \pmod 5$, $x \equiv 1 \pmod 3$

no soluzioni, due equazioni incompatibili

[parentesi....

$x \equiv 5 \pmod{18} \iff$ $\begin{cases} x \equiv ? \pmod 3 \\ x \equiv ? \pmod 3 \\ x \equiv ? \pmod 2 \end{cases}$ no

$\begin{cases} x \equiv ? \pmod 9 \\ x \equiv ? \pmod 2 \end{cases}$]

4) $\begin{cases} x \equiv 8 \ (21) \\ x \equiv 14 \ (15) \end{cases}$

$x \equiv 8 \equiv 1 \ (7)$
$x \equiv 8 \equiv 2 \ (3)$
$x \equiv 14 \equiv 4 \ (5)$
$x \equiv 14 \equiv 2 \ (3)$

$\Leftrightarrow \begin{cases} x \equiv 1 \ (7) \\ x \equiv 2 \equiv -1 \ (3) \\ x \equiv 4 \equiv -1 \ (5) \end{cases}$

$\equiv -1 \ (15) \quad \equiv 7$

14	0
29	1
44	2
59	3
74	4
⋮	⋮

$\begin{cases} x \equiv 1 \ (7) \\ x \equiv -1 \ (15) \end{cases} \Leftrightarrow x \equiv 29 \ (105)$

$7^{-3} \equiv ?$ mod 13

Troviamo 7^{-1}, cioè

y t.c. $7y \equiv 1$ (13)

$7 \cdot 1 = 7 \neq 1$

$7 \cdot 2 = 14 \equiv 1$ ok! $y = 2$

3^{-1} mod 13

$3 \cdot 1 = 3$

$3 \cdot 2 = 6$

$3 \cdot 3 = 9$

$3 \cdot 4 \equiv 12$

$3 \cdot 5 \equiv 15 \equiv 2$

$18 \equiv 5$

$21 \equiv 8$

$24 \equiv$

$3 \cdot$ qualcosa $=$ (multiplo di 13) $+1$

$3 \cdot$ qualcosa $= 13+1$ no!

$3 \cdot$ qualcosa $\equiv 26+1$ ok! $3 \cdot 9$

$\Rightarrow \boxed{3^{-1} = 9}$

Quindi, le soluzioni di $(S)\begin{cases}(i)\\(ii)\end{cases}$ sono

$$\{x \mid x \equiv 29 \bmod 105 \text{ oppure } x \equiv 71 \bmod 105\}$$

$$\{29+105k \mid k \in \mathbb{Z}\} \cup \{71+105k \mid k \in \mathbb{Z}\}$$

Es: Trovare tutti gli $x \in \mathbb{Z}$ tali che

$$6^x \equiv 4 \pmod{19}$$

In generale, a che cosa sono congrui $6^0, 6^1, 6^2, 6^3, \ldots$

6^0	6^1	6^2	6^3	6^4	6^6	6^9	6^{10}	6^{11}	6^{12}	6^{13}	6^{18}
1	6	$17 \equiv -2$	7	4	*	11	*	*	1	6	-2	7	4	1

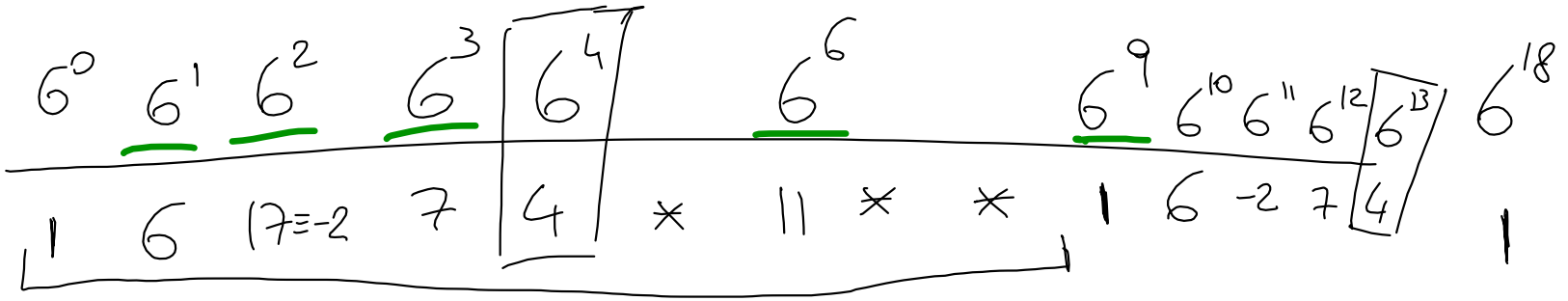
$6^6 \equiv 6^4 \cdot 6^2 \equiv 4 \cdot (-2) \equiv -8$ $\quad$ $6^9 \equiv 6^6 \cdot 6^3 \equiv 11 \cdot 7 = 77 \equiv 20 \equiv 1$

$\Rightarrow 6^4, 6^{13}, 6^{22}, \dots 6^{9k+4}$ sono tutti congrui a 4 mod 9

$6^{-5} \equiv (6^{-1})^5 \equiv 4$

dev'essere per forza così, perché $6^{-5} \cdot 1 \equiv 6^{-5} \cdot 6^9 \equiv 6^4 \equiv 4$

Chi mi dice che non ci sia un altro 4 negli asterischi?



Supponiamo che $6^7 \equiv 4$ $6^4 \equiv 4$ $6^3 \equiv \frac{6^7}{6^4} \equiv \frac{4}{4} = 1$

impossibile, perché so che il primo 1 sta in 9

Teorema: quando faccio potenze modulo un primo, $a^0, a^1, a^2, \ldots$

1) a un certo punto trovo un 1
2) il primo 1 è su un divisore di $p-1$
3) i numeri tra $a^0=1$ e il primo 1 sono tutti diversi

Dim: 1, 2. già li sapete

3) Se $a^m \equiv a^n$ con $0 < m < n <$ posizione del primo 1

allora $a^{n-m} \equiv \frac{a^n}{a^m} \equiv 1$, e $0 < n-m <$ posizione del primo 1.

assurdo!

$\Rightarrow$ la sol. dell'esercizio è $X \equiv 4 \mod 9$

$6^{356} \mod 19$

$*$

$6^{\text{quello che fa } 356 \mod 19}$

Altro fenomeno che può succedere poendo fatte congruenze esponenziali:

$6^x \mod 16$

$6^x \equiv ? \mod 16$

6^{-1}	6^0	6^1	6^2	6^3	6^4	6^5	...
non esiste!	1	6	4	8	0	0	0 ...

0 da questo punto in poi

Succede quando avere

$a^x \mod p^h$ e a è multiplo di p

(Unico caso in cui congruenze esponenziali $\neq$ congruenze mod ordine)

$6^x \equiv 4 \mod 19 \cdot 16$ sse

$6^x \equiv 4 \mod 19 \iff x \equiv 4 \mod 9$

$6^x \equiv 4 \mod 16 \iff x = 2$ e basta!

note per domande dopo la lezione

per quali numeri

$x^3 = 1 \mod 19$

(*) $396x + (105 \cdot k)y = 234$

$ax + by = c$ quando ha sol?

se $\mathrm{mcd}(a,b) \mid c$

ha sol. se $\mathrm{mcd}(396, (105k)) \mid 234$

$9 \cdot 44 = 3^2 \cdot 4 \cdot 11$ $\quad 3 \cdot 5 \cdot 7 \cdot k$ $\quad 9 \cdot 2 \cdot 13$