Università degli Studi di Roma "Tor Vergata"

CdL in Ingegneria Informatica

corso di "Algebra e Logica" (prof. Fabio Gavarini)

Tutorato su ARITMETICA MODULARE e SISTEMI di EQUAZIONI CONGRUENZIALI

.... $*$ ....

1 — Risolvere il sistema di equazioni congruenziali

$$\circledast : \begin{cases} -25\,x \equiv 14^{64938} & (\bmod 11) \\ 47\,x \equiv 436 & (\bmod 6) \end{cases}$$

2 — Calcolare tutte le soluzioni del sistema di equazioni congruenziali seguente:

$$\circledast : \begin{cases} 21\,x \equiv -93 & (\bmod 4) \\ -11\,x \equiv 39 & (\bmod 7) \\ 6179\,x \equiv 983 & (\bmod 3) \\ 71\,x \equiv 52 & (\bmod 5) \end{cases}$$

3 — Calcolare tutte le soluzioni in $\mathbb{Z}$ del sistema di equazioni congruenziali

$$\circledast : \begin{cases} 17\,x \equiv -105 & (\bmod 5) \\ -55\,x \equiv 11 & (\bmod 3) \\ 23\,x \equiv 36 & (\bmod 7) \end{cases}$$

4 — Calcolare il resto di $N := 435^{159}$ nella divisione per 21.

5 — Calcolare il resto di $N := 53407617^{85043175}$ nella divisione per 12.

6 — Determinare tutti i numeri interi $x \in \mathbb{Z}$ per i quali si abbia *simultaneamente*

$$-93 \cdot x \equiv 378 \;\; (\bmod 15) \qquad \text{e} \qquad \overline{215} \cdot \overline{x} = -\overline{24} \quad \text{in } \mathbb{Z}_7$$

7 — Calcolare le ultime due cifre decimali di $7^{6503219}$.

8 — *(a)* Determinare — se esiste — il più piccolo valore di $x \in \mathbb{Z}$ tale che

$$x \equiv 543^{80431} \pmod{20} \qquad \text{e} \qquad 35 \leq x \leq 78$$

(b) Calcolare tutte le soluzioni dell'equazione modulare $\overline{-317}\,\overline{x} = \overline{543^{80431}}$ nell'anello $\mathbb{Z}_{20}$ delle classi resto modulo 20 .

9 — Risolvere l'equazione congruenziale $127\,x \equiv -419 \pmod{30}$ mediante la risoluzione di un opportuno sistema di tre equazioni congruenziali.

10 — Determinare tutte le soluzioni del sistema di equazioni congruenziali

$$\circledast : \begin{cases} -18\,x \equiv 32 & (\bmod\ 5) \\ 145\,x \equiv 55 & (\bmod\ 20) \\ 237\,x \equiv -42 & (\bmod\ 9) \end{cases}$$

11 — Determinare tutti i numeri interi $x \in \mathbb{Z}$ per i quali si abbia *simultaneamente*

$$[381]_{15} \cdot [\,x\,]_{15} = -[132]_{15} \quad \text{in } \mathbb{Z}_{15} \qquad \text{e} \qquad [95]_7 \cdot [\,x\,]_7 = -[61]_7 \quad \text{in } \mathbb{Z}_7$$

12 — Per ogni $z \in \mathbb{Z}$, dimostrare che si ha $[\,z\,]_{35} \in U(\mathbb{Z}_{35})$ se e soltanto se si ha $[\,z\,]_5 \in U(\mathbb{Z}_5)$ e $[\,z\,]_7 \in U(\mathbb{Z}_7)$.

13 — Calcolare il resto di 865^{70396} nella divisione per 21, per 7 e per 3 .

14 — Calcolare il resto di 976^{69518} nella divisione per 30, per 5 e per 6 .

15 — Calcolare il resto nella divisione per 20 dei tre numeri

$$a := 457^{35062867} \quad , \qquad b := 2384^{16} \quad , \qquad c := 645^{5607290843}$$
