AL 1
Esercizi per casa, III prova
Soluzioni

1(a) Dato che $\mathrm{MCD}(12, 16) = 4$ divide 8, la congruenza è risolubile ed ha esattamente 4 soluzioni distinte modulo 16. La congruenza è equivalente alla congruenza $3X \equiv 2 \mod 4$, che ha la soluzione $x_0 = 2$ (soluzione unica $\mod 4$). Le soluzioni non congrue $\mod 16$ sono quindi $x_k = x_0 + 4k$, $k = 0, 1, 2, 3$ cioè $2, 6, 10, 14$.

1(b) L'unica soluzione modulo 55 è 26

1(c) La congruenza ha 7 soluzioni distinte modulo 35 e precisamente $4, 9, 14, 19, 24, 29, 34$.

1(d) La congruenza ha 120 soluzioni distinte modulo 840, date da $3+7k$ con $k \in \mathbb{Z}$, $0 \leq k \leq 119$.

2(a) Il sistema è risolubile perché $\mathrm{MCD}(7, 11) = 1$. Per sostituzione: dalla prima congruenza ricaviamo $x = 5 + 7h$, $h \in \mathbb{Z}$. Sostituendo nella seconda $5 + 7h \equiv 7 \mod 11$, quindi $7h \equiv 2 \mod 11$, cioè $h \equiv 5 \mod 11$. Pertanto, $h = 5 + 11k$,$k \in \mathbb{Z}$ e $x = 5 + 7(5 + 11k) = 40 + 77k$. Ne segue che 40 è l'unica soluzione del sistema dato modulo 77. Con la formula utilizzata per dimostrare il teorema cinese dei resti: $x = 5 \cdot 11 \cdot 11^* + 7 \cdot 7 \cdot 7^*$, dove 11^* è l'inverso aritmetico di 11 modulo 7 e 7^* è l'inverso aritmetico di 7 modulo 11. Cioè $11^* = 2$ e $7^* = 8$. Quindi $x = 5 \cdot 11 \cdot 2 + 7 \cdot 7 \cdot 8 = 502 \equiv 40 \mod 77$.

2(b) La soluzione è 559 modulo 2244.

2(c) La soluzione è 52 modulo 32736.

3(a) La soluzione è 54 modulo 56.

3(b) La soluzione è 601 modulo 1001

3(c) La soluzione è 185 modulo 429 (e quindi $185, 614, 1043, 1472, 1901, 2330$ modulo $9 \cdot 13 \cdot 22 = 2574$)

4(a) Osserviamo prima di tutto che $7^4 \equiv 1 \mod 10$. Quindi se troviamo b tale che $7^7 = b + 4k$ (per qualche $k \in \mathbb{Z}$) otteniamo che $7^{(7^7)} = 7^{(b+4k)} = 7^b \cdot 7^{4k} \equiv 7^b \mod 10$, dato che $7^{4k} = (7^4)^k \equiv 1^k \equiv 1 \mod 10$. Si osserva facilmente che $b = 3$, perché $7^2 \equiv 1 \mod 4$ e quindi $7^7 = 7^2 \cdot 7^2 \cdot 7^2 \cdot 7 \equiv 7 \equiv 3 \mod 4$. Ne segue che $7^{(7^7)} \equiv 7^3 \equiv 3 \mod 10$.

4(b) Per il Teorema di Wilson, $28! \equiv -1 \mod 29$, quindi $26! \equiv -1 \cdot 28^* \cdot 27^* \mod 29$, dove 28^* e 29^* sono gli inversi aritmetici di 28 e 27 modulo 29. Si verifica facilmente che $27^* \equiv 14 \mod 29$ e $28^* \equiv -1 \mod 29$. Pertanto, $26! \equiv 14 \mod 29$.

4(c) Per il "Piccolo Teorema di Fermat", si ha $(a^p)^q \equiv a^p \mod q$ e quindi, dato che per ipotesi $a^p \equiv a \mod q$, si ottiene $(a^p)^q \equiv a \mod q$. Analogamente $(a^p)^q \equiv a \mod p$. Ne segue che $(a^p)^q \equiv a \mod pq$, dato che p e q sono coprimi.