SOLUZIONI DELL' ESAME DI METÀ SEMESTRE

1. Si determinino tutte le soluzioni intere della seguente equazione: $2X+3Y+5Z=100$.

SOLUZIONE. *Dalla Teoria sappiamo che se* (x_1, x_2) *è una particolare soluzione di* $2X_1+(3,5)X_2 = 100$ *e* (y_1, y_2) *è una particolare soluzione di* $3Y_1 + 5Y_2 = (3,5)$. *Allora tutte e sole le soluzioni di questa equazioni si scrivono nel seguente modo:*

$$\begin{aligned} x = &\quad x_1 + t \\ y = &\quad y_1x_2 - 2y_1t + 5s \\ z = &\quad y_2x_2 - 2y_2t - 3s \end{aligned}$$

al variare di $s, t \in \mathbf{Z}$. *Nel nostro caso possiamo prendere* $(x_1, x_2) = (40, 20)$ *e* $(y_1, y_2) = (2, -1)$ *e otteniamo le soluzioni:*

$$\begin{aligned} x = &\quad 40 + t \\ y = &\quad 40 - 4t + 5s \\ z = &\quad -20 + 2t - 3s. \end{aligned}$$

2. Per quali valori del parametro λ il seguente sistema di congruenze ammette un unica soluzione? $\begin{cases} 2x - 4y \equiv 0 \bmod 7 \\ 3x + \lambda^2 y \equiv 1 \bmod 7. \end{cases}$

SOLUZIONE. *Dalla teoria segue che il sistema di congruenze in questione ammette un unica soluzione se e solo se il determinante della matrice* $\begin{pmatrix} 2 & -4 \\ 3 & \lambda^2 \end{pmatrix}$ *non è congruente a* 0 *modulo* 7. *Quindi se e solo se* $2\lambda^2+12 \not\equiv 0 \bmod 7$ *o analogamente se e solo se* $\lambda^2 \not\equiv 1 \bmod 7$ *il che vuol dire* $\lambda \not\equiv \pm 1 \bmod 7$.

3. Dimostrare il piccolo Teorema di Fermat.

SOLUZIONE. *Vedere le note a pagina 28*

4. Dimostrare che per ogni primo p la seguente congruenza è verificata: $(p-4)! \equiv 6^* \bmod p$ dove 6^* è l'inverso aritmetico modulo p.

SOLUZIONE. *Dal Teorema di Wilson che afferma che* $(p-1)! \equiv -1 \bmod p$, *deduciamo che* $-1 \equiv (p-1)(p-2)(p-3)\cdot(p-4)! \equiv -6(p-4)! \bmod p$. *Moltiplicando entrambi i membri della congruenza per* -6^*, *otteniamo* $6^* \equiv 6^* \cdot 6(p-4)! \equiv (p-4)! \bmod p$.

5. Calcolare il numero delle soluzioni modulo 125 della seguente congruenza polinomiale: $X^3 - 11X^2 + 24X - 14 \equiv 0 \bmod 125$.

SOLUZIONE. *Cominciamo osservando che la congruenza* $f(X) := X^3 - 11X^2 + 24X - 14 \equiv 0 \bmod 5$ *ha come soluzioni* $x = 1, 4$. *Inoltre* $f'(1) = 5$ *e* $f'(4) = -16 \not\equiv 0 \bmod 5$. *Dal Teorema del sollevamento otteniamo subito che* $x = 4$ *da luogo ad un unica soluzione* $x_1 = 24$ *modulo* 25 *e* x_1 *da luogo ad un unica soluzione* $y_1 = 74$ *modulo* 125. *Per quanto riguarda la soluzione* $x = 1$, *osserviamo che* $f(1) = 0$ *e pertanto* $x = 1$ *da luogo a* 5 *soluzioni modulo* 25 *che sono* $1, 6, 11, 16, 21$. *Adesso osserviamo che* $f(1) = 0, f(6) = -50, f(11) = 250, f(16) = 1650, f(21) = 4900$ *e* $f(6), f(16), f(21) \not\equiv 0 \bmod 125$. *Pertanto* 1 *e* 11 *sono le uniche soluzioni modulo* 25 *che danno luogo a (cinque ciascuna) soluzioni modulo* 125. *In conclusione la congruenza ammette* $1 + 5 + 5 = 11$ *soluzioni.*

6. Calcolare le soluzioni del sistema $\begin{cases} X \equiv 4 \bmod 5 \\ X \equiv 3 \bmod 7 \end{cases}$ nell'intervallo $[100, 250]$.

SOLUZIONE. *Si tratta di un applicazione del Teorema Cinese dei resti dal quale si deduce che l'equazione in questione ammette un unica soluzione modulo* 35. *Usando la formula di risoluzione si calcola subito che la soluzione è* $x = 24$. *Gli interi* $y \equiv 24 \bmod 35$ *nell'intervallo* $[100, 250]$ *sono* $129, 164, 199, 234$.

7. Si enunci il Teorema del sollevamento per soluzioni di congruenze polinomiali.

SOLUZIONE. *Sia* $f \in \mathbf{Z}[X]$, $f \neq 0$; *sia* p *un numero primo e* $n \in \mathbf{N}$. *Ogni soluzione* y *della congruenza*

$$f(X) \equiv 0 \bmod p^{n+1} \tag{1}$$

ha la forma $y = x + tp^n$ *dove* $0 \leq t < p$ *e* x *è una soluzione di* $f(X) \equiv 0 \bmod p^n$. *Inoltre Inoltre*

- *Se* $f'(x) \not\equiv 0 \bmod p$, *allora* $x + tp^n$ *risolve (1) se e solo se* $t \equiv \frac{-f(x)}{(p^n f'(x))} \bmod p$;
- *Se* $f'(x) \equiv 0 \bmod p$ *e* $f(x) \not\equiv 0 \bmod p^{n+1}$, *allora* $x + tp^n$ *non è mai una soluzione di (1);*
- *Se* $f'(x) \equiv 0 \bmod p$ *e* $f(x) \equiv 0 \bmod p^{n+1}$, *allora* $x + tp^n$ *è una soluzione di (1) per ogni* $0 \leq t < p$.

8. Sia p un primo dispari tale che $q = 2p + 1$ è anche primo. Mostrare che se un intero a, $2 \leq a \leq p - 2$ è tale che $a^p \equiv -1 \bmod q$ se e solo se a è una radice primitiva modulo q.

SOLUZIONE. a^p è una soluzione della congruenza $X^2 - 1 \equiv 0 \bmod q$. Quindi in ogni caso $a^p \equiv \pm 1 \bmod q$. Chiaramente se a è una radice primitiva modulo q, allora non si può

avere $a^p \equiv 1 \bmod q$ (altrimenti si avrebbe $\mathrm{ord}_q(a)|p$) e quindi deve essere $a^p \equiv -1 \bmod q$. Viceversa se a non fosse una radice primitiva allora $\mathrm{ord}_q(a) < 2p$ implicherebbe $\mathrm{ord}_q(a) \in \{1, 2, p\}$. Ma $\mathrm{ord}_q(a) \neq 1, 2$ perchè $a \neq 1, p-1$. Infine $\mathrm{ord}_q(a) \neq p$ perchè altrimenti si avrebbe $a^p \equiv 1 \bmod q$.

9. *Quante e quali soluzioni ha la congruenza* $X^{15} \equiv 5 \bmod 93$? *Suggerimento: lavorare modulo primi*

SOLUZIONE. *La congruenza ha soluzione se e solo se le due congruenze:* $X^{15} \equiv 5 \bmod 31$ *e* $X^{15} \equiv 5 \bmod 3$ *sono entrambe risolubili. Per il Criterio di Eulero la prima congruenza non è risolubile infatti* $5^{(31-1)/(30,15)} = 25 \not\equiv 1 \bmod 31$. *Pertanto nemmeno la congruenza modulo* 93 *è risolubile.*

10. Mostrare direttamente che non esiste una radice primitiva modulo 24.

SOLUZIONE. *Gli elementi di* $\mathbf{Z}/24\mathbf{Z}$ *coprimi con* 24 *sono* $1, 5, 7, 11, 13, 17, 19$ *e* 23 *che tutti hanno ordine* 2 *tranne il primo che ha ordine* 1. *Pertanto nessuno ha ordine* $\varphi(24) = 8$.

11. Illustrare l'algoritmo di Gauss per il calcolo di una radice primitiva.

SOLUZIONE. *ALGORITMO DI GAUSS*

`passo 1` Scegliere $a \in \mathbf{Z}/p\mathbf{Z}^*$ con $a \neq 1$ e calcolare $d :=\mathrm{ord}_p(a)$.
Se $d = p-1$, allora **OUTPUT:** a è una radice primitiva, **END**.

`passo 2` Scegliere $b \in \mathbf{Z}/p\mathbf{Z}^*$ con $b \neq 1$ tale che $b \not\equiv a^i \bmod p, \forall i = 1, \ldots, d$ e calcolare $t :=\mathrm{ord}_p(b)$.
Se $t = p-1$, allora **OUTPUT:** a è una radice primitiva, **END**.

`passo 3` Sia $d_1 =\mathrm{mcm}(t, d)$ e sia $a_1 \equiv a^{d/(d,t)}b \bmod p$. (Nota che $\mathrm{ord}_p(a_1) = d_1$)
Se $d_1 = p-1$, allora **OUTPUT:** a_1 è una radice primitiva, **END**.

`passo 4` Vai al passo 2.

12. Usare una radice primitiva per mostrare che se p è primo e m è un intero, allora

$$1^m + 2^m + \cdots + (p-1)^m \equiv \begin{cases} 0 \bmod p & \text{se } (p-1) \not| m \\ -1 \bmod p & \text{se } p-1|m. \end{cases}$$

SOLUZIONE.*Sia* g *una radice primitiva modulo* p. *Si ha che*

$$\sum_{j=1}^{p-1} j^m \equiv \sum_{i=1}^{p-1} g^{im} \bmod p.$$

Se $p-1|m$, *allora* $g^m \equiv 1 \bmod p$. *Dunque*

$$\sum_{i=1}^{p-1} g^{im} \equiv p-1 \equiv -1 \bmod p.$$

Se invece $p-1 \not| m$, *allora* $g^m \not\equiv 1 \bmod p$ *e*

$$\sum_{i=1}^{p-1} g^{im} = \frac{g^{pm}-g^m}{g^m-1} \equiv \frac{g^m-g^m}{g^m-1} \equiv 0 \bmod p.$$