# Stage/Campionato Urbi et Orbi

## Equazioni diofantee e congruenze

29 Novembre 2019

*Soluzioni scritte da* **Luca Vantaggio, L.S.S. "Giuseppe Battaglini", TARANTO**.

Potrai trovare tutto il materiale didattico dello stage **(lezioni,testi,gare,risultati)** linkato alla pagina

**http://www.problemisvolti.it/ZStageMateriale.html**

Invece, potrai trovare l'elenco delle squadre iscritte al campionato *Stage Urbi et Orbi* linkato alla pagina:

**http://www.problemisvolti.it/StageOlimpiadiMatematica.html**

*Nota:* da ora in poi la soluzione di ogni esercizio sarà denotata con $s$.

**Esercizio 1.** Una pulce e un grillo saltano sulla retta dei numeri. La pulce parte da 0 e fa salti lunghi 17 unità, mentre il grillo parte da 1 e fa salti di 13 unità. Qual è il più piccolo numero positivo che può essere toccato da entrambi?

Evidentemente la soluzione $s$ è il minimo intero positivo che risolve il seguente sistema di congruenze:

$$\begin{cases} x \equiv 0 \mod 17 \\ x \equiv 1 \mod 13 \end{cases}$$

che è equivalente a

$$\begin{cases} x \equiv -51 \mod 17 \\ x \equiv -51 \mod 13 \end{cases}$$

e dunque, per il teorema cinese del resto, deve valere che $s \equiv -51 \mod 17 \cdot 13$ giacché 13 e 17 sono coprimi. Di conseguenza $s \equiv -51 \mod 221$ e quindi $s = 170$.
**170**

**Esercizio 2.** Una pulce e un grillo saltano sulla retta dei numeri. La pulce parte da 0 e fa salti lunghi 747 unità, mentre il grillo parte da 26 e fa salti di 350 unità. Qual è il più piccolo numero positivo che può essere toccato da entrambi?

Come prima risulta che $s$ è il minimo intero positivo che è soluzione del seguente sistema di congruenze:

$$\begin{cases} x \equiv 0 \mod 747 \\ x \equiv 26 \mod 350 \end{cases}$$

La prima congruenza del sistema è di fatto equivalente alla condizione $747|x$, da cui non è riduttivo porre $x = 747y$ con $y$ intero e ci chiediamo dunque quando $747y \equiv 26 \mod 350$.

$$747y \equiv 26 \mod 350 \Leftrightarrow 47y \equiv 26 \mod 350$$

Da $M.C.D.(47, 350) = 1$ si ottiene che esiste un'unica classe di resto modulo 350 che è soluzione della precedente congruenza, ed è la classe di resto di un qualsiasi $\alpha$ intero per cui esiste un $\beta$ intero tale che $47\alpha + 350\beta = 26$.

Sfruttando l'algoritmo delle divisioni ripetute o algoritmo di Euclide si giunge alla soluzione $(\alpha_0, \beta_0) = (-67 \cdot 26, 9 \cdot 26)$, da cui $y \equiv -67 \cdot 26 \mod 350$ e quindi

$$\begin{cases} x \equiv -67 \cdot 26 \cdot 747 \mod 747 \\ x \equiv -67 \cdot 26 \cdot 747 \mod 350 \end{cases}$$

e quindi $x \equiv -67 \cdot 26 \cdot 747( \mod 747 \cdot 350)$ visto che $M.C.D.(747, 350) = 1$. Perciò $x \equiv -1742 \cdot 747 \mod 747 \cdot 350$ è equivalente al sistema iniziale. Da ciò, con un semplice computo, si ottiene che $s = 8 \cdot 747 = 5976$.
**5976**

**Esercizio 3.** Trovare la somma di tutti gli eventuali interi $x$, compresi tra 0 e 42, che soddisfano la condizione $6x \equiv 18 \mod 43$.

Da $M.C.D.(6, 43) = 1$ si ottiene che $6x \equiv 18 \mod 43 \Leftrightarrow x \equiv 3 \mod 43$ e quindi $s = 3$.
**3**

**Esercizio 4.** Siano $a$,$b$ due cifre del numero $n = 250a10b315576$. Se $n$ è divisibile per 99, quanto vale $10a + b$?

Chiaramente $99|n$ se e solo se $9|n$ e $11|n$ (si può vedere o con il teorema cinese del resto o con la definizione astratta di minimo comune multiplo). Ma, per i ben noti criteri di congruenza, risulta che le precedenti condizioni sono equivalenti al seguente sistema di congruenze:

$$\begin{cases} 2+5+0+a+1+0+b+3+1+5+5+7+6 \equiv 0 \mod 9 \\ 2-5+0-a+1-0+b-3+1-5+5-7+6 \equiv 0 \mod 11 \end{cases}$$

da cui risulta che

$$\begin{cases} a+b \equiv -1 \mod 9 \\ -a+b \equiv 5 \mod 11 \end{cases}$$

Notando che $10 \equiv 1 \mod 9$ e $10 \equiv -1 \mod 11$ si ottiene che il precedente sistema di congruenze è equivalente a

$$\begin{cases} 10a+b \equiv -1 \mod 9 \\ 10a+b \equiv 5 \mod 11 \end{cases}$$

da cui

$$\begin{cases} 10a+b \equiv 71 \mod 9 \\ 10a+b \equiv 71 \mod 11 \end{cases}$$

e quindi $10a + b \equiv 71 \mod 99$ per il teorema cinese del resto. Di conseguenza $s = 10a + b = 71$ visto che $10a + b$ è un numero di due cifre.
**71**

**Esercizio 5.** Trovare la somma di tutti gli eventuali interi $x$, compresi fra 0 e 41, che soddisfano la condizione $6x \equiv 18 \mod 42$.

Da $M.C.D.(6, 42) = 6|18$ si ottiene che la congruenza ammette soluzioni e in particolare le classi di resto che la risolvono sono 6. E' evidente che siffatte classi di resto si ottengono tenendo in considerazione che $6x \equiv 18 \mod 42 \Leftrightarrow x \equiv 3 \mod 7$, da cui evidentemente $s = 3+(3+7)+(3+2\cdot 7)+(3+3\cdot 7)+(3+4\cdot 7)+(3+5\cdot 7) = 3\cdot 6+(1+2+3+4+5)\cdot 7 = 18 + 15 \cdot 7 = 123$.
**123**

**Esercizio 6.** Trovare la somma di tutti gli eventuali interi $x$, compresi fra 0 e 41, che soddisfano la condizione $6x \equiv 15 \mod 42$.

Da $M.C.D.(6, 42) = 6$ che non divide 15 si ottiene che la suddetta congruenza non ammette soluzioni.
**0**

**Esercizio 7.** Una nota canzone dell'isola *Kenoncè*, anziché raccontare (come nel resto del mondo) di 44 gatti in fila per 6 col resto di 2, racconta di $n$ gatti (con $8000 < n < 9500$) che in fila per 7 danno il resto di 5 mentre in fila per 11 e per 13 danno sempre resto di 0. Quanto vale $n$? Se tale $n$ non esiste dare come risposta 0 mentre se non fosse univocamente determinato dare come risposta 9999.

Di fatto ci viene chiesto di determinare (se esiste ed è unica) la soluzione $n \in ]8000, 9500[$ del seguente sistema di congruenze:

$$\begin{cases} x \equiv 5 \mod 7 \\ x \equiv 0 \mod 11 \\ x \equiv 0 \mod 13 \end{cases}$$

Come nell'esercizio 2 poniamo (senza perdita di generalità) $x = 11 \cdot 13y$ con $y$ intero e ci chiediamo quando $11 \cdot 13y \equiv 5 \mod 7$. E' necessario un breve computo per determinare che $y \equiv 4 \mod 7$ e quindi, per il teorema cinese del resto, il precedente sistema di congruenze è equivalente a $x \equiv 11 \cdot 13 \cdot 4 \mod 7 \cdot 11 \cdot 13$, e a questo punto non è difficile vedere che $n$ esiste, è unico ed è pari a 8580.
**8580**

**Esercizio 8.** Una pulce, un grillo e una cavalletta saltano sulla retta dei numeri. La pulce parte da 0 e fa salti lunghi 23 unità, il grillo parte da 1 e fa salti di 17 unità mentre la cavalletta parte da $-1$ e fa salti di 19 unità. Qual è il più piccolo intero positivo che può essere toccato da tutti e tre?

In pratica ci viene chiesto il minimo intero positivo $s$ che è soluzione del seguente sistema di congruenze:

$$\begin{cases} x \equiv 0 \mod 23 \\ x \equiv 1 \mod 17 \\ x \equiv -1 \mod 19 \end{cases}$$

che, grazie all'equivalenza tra le ultime due congruenze con la congruenza $x \equiv 18 \mod 17 \cdot 19$ (per il teorema cinese del resto), può opportunamente venir riscritto come

$$\begin{cases} x \equiv 0 \mod 23 \\ x \equiv 18 \mod 323 \end{cases}$$

A questo punto, con gli stessi metodi usato nell'esercizio 2, si ottiene che

$$\begin{cases} x \equiv 1633 \mod 23 \\ x \equiv 1633 \mod 323 \end{cases}$$

che è equivalente a $x \equiv 1633 \mod 7429$, da cui $s = 1633$.
**1633**

**Esercizio 9.** Una pulce, un grillo e una cavalletta saltano sulla retta dei numeri come nel problema **8**. Qual è la minima distanza tra due punti distinti che possano essere toccati da tutti e tre?

Per quanto visto nel precedente problema, tutti e soli punti che possono essere raggiunti da tutti e tre sono i valori interi $x$ tali che $x \equiv 1633 \mod 7429$, da cui la minima distanza è proprio 7429.
**7429**

**Esercizio 10.** Trovare la cifra delle unità di $2013^{2019}$.

Poiché $s$ è il resto di $2013^{2019}$ dalla divisione per 10, si ha che $2013^{2019} \equiv s \mod 10$, che per il teorema cinese del resto è equivalente a

$$\begin{cases} 2013^{2019} \equiv s \mod 2 \\ 2013^{2019} \equiv s \mod 5 \end{cases}$$

Da $\phi(5) = 4$, per il teorema di Eulero-Fermat, si ottiene che

$$\begin{cases} 1 \equiv s \mod 2 \\ 3^3 \equiv s \mod 5 \end{cases}$$

e quindi

$$\begin{cases} s \equiv 7 \mod 2 \\ s \equiv 7 \mod 5 \end{cases}$$

e dunque $s \equiv 7 \mod 10$, da cui $s = 7$.
**7**

**Esercizio 11.** Trovare le ultime due cifre di $1997^{2009}$.

Come prima scriviamo che

$$\begin{cases} 1997^{2009} \equiv s \mod 4 \\ 1997^{2009} \equiv s \mod 25 \end{cases}$$

da cui

$$\begin{cases} s \equiv 1 \mod 4 \\ s \equiv (-3)^9 \mod 25 \end{cases}$$

in quanto $\phi(25) = 10$. Il precedente sistema di congruenze si dimostra essere equivalente (dopo un po' di conti) a

$$\begin{cases} s \equiv 17 \mod 4 \\ s \equiv 17 \mod 25 \end{cases}$$

e quindi $s = 17$.
**17**

**Esercizio 12.** Calcolare il resto dalla divisione di $2^{1198765432104}$ per 26.

Come prima, sfruttando il teorema cinese del resto, possiamo scrivere

$$\begin{cases} 2^{1198765432104} \equiv s \mod 2 \\ 2^{1198765432104} \equiv s \mod 13 \end{cases}$$

che, poiché $1198765432104 \equiv 0 \mod 12 = \phi(13)$, è equivalente a

$$\begin{cases} 0 \equiv s \mod 2 \\ 1 \equiv s \mod 13 \end{cases}$$

e quindi

$$\begin{cases} 14 \equiv s \mod 2 \\ 14 \equiv s \mod 13 \end{cases}$$

da cui, per il teorema cinese del resto, si ottiene $s = 14$.
**14**

**Esercizio 13.** Trovare il massimo fra tutti i numeri che compaiono come ascissa o come ordinata di un punto a coordinate intere che soddisfa l'equazione $40x^2 + 21y^2 - 58xy - 29 = 0$.

Notando che $40x^2+21y^2-58xy = 40x^2+21y^2-28xy-30xy = 4x\cdot 10x+3y\cdot 7y-4x\cdot 7y-10x\cdot 3y = (4x-3y)(10x-7y)$ si ottiene che l'equazione di partenza può essere riscritta come $(4x-3y)(10x-7y) = 29$. Sfruttando la primalità di 29 è facile determinare tutte le coppie $(x, y)$ a coordinate intere (basta porre un fattore pari a $\pm 1$ e l'altro pari a $\pm 29$), e si ottiene che sono $(40, 53), (-40, -53), (100, 143)$ e $(-100, -143)$. Di conseguenza $s = 143$.
**143**

**Esercizio 14.** Una pulce salta sulla retta dei numeri. Parte da 0 e deve raggiungere 1 facendo solo salti di lunghi $77, 91$ o 143. Qual è il numero minimo di salti che deve fare se quelli da 143 può farli solo in avanti?

In pratica ci viene chiesto qual è il valore minimo di $|x| + |y| + |z|$ con $z \geq 0$ e $(x, y, z)$ soluzione di componenti intere dell'equazione $77x + 91y + 143z = 1$. Sapendo che tutte le soluzioni dell'omogenea $77\alpha + 91\beta + 143\gamma = 0$ sono tutte e le sole terne $(13x_1, 11y_1, 7z_1)$ con il vincolo $x_1 + y_1 + z_1 = 0$ e notando che $(1, -18, 12)$ è soluzione dell'equazione di partenza, si ottiene che tutte le soluzioni dell'equazione dell'esercizio sono della forma $(1+13x_1, -18+11y_1, 12-7x_1-7y_1)$. A questo punto non è difficile notare che quella che minimizza la somma dei valori assoluti delle componenti è $(1, -7, 5)$ e quindi $s = 13$.
**13**

**Esercizio 15.** Attorno alla stella *Lucente* ruotano nello stesso verso con velocità costanti su orbite circolari (aventi *Lucente* come centro e che giacciono sullo stesso piano) tre pianeti: *Bingo,Bango* e *Bongo*. Sapendo che i periodi di rivoluzione dei tre pianeti sono rispettivamente $24, 88$ e 152 anni terrestri e che, ad un certo istante, giacciono tutti sulla stessa semiretta avente origine in *Lucente*, dire quanto vale, misurato in anni terrestri, il minimo intervallo di tempo che deve trascorrere prima che i tre pianeti giacciano di nuovo tutti su una semiretta avente origine in *Lucente*.

Chiamiamo $\omega_1, \omega_2$ e $\omega_3$ le velocità angolari dei suddetti pianeti misurate in $(\textit{anni terrestri})^{-1}$. Evidentemente $\omega_1 = \frac{360°}{24}, \omega_2 = \frac{360°}{88}$ e $\omega_3 = \frac{360°}{152}$. Poiché, dopo un intervallo di tempo $t$ due pianeti di velocità angolari $a$ e $b$ si ritroveranno allineati su una semiretta come in partenza se e solo se vale che $at - bt = 360°x$ con $x$ intero, necessariamente tutti e tre i pianeti si troveranno allineati su una semiretta con origine in *Lucente* se e solo se

$$\begin{cases} (\omega_1 - \omega_2)t = k \cdot 360° \\ (\omega_2 - \omega_3)t = p \cdot 360° \end{cases}$$

dove $t$ è il tempo trascorso e $k, p$ sono numeri interi. Di conseguenza abbiamo che

$$\begin{cases} (\frac{360°}{24} - \frac{360°}{88})t = k \cdot 360° \\ (\frac{360°}{88} - \frac{360°}{152})t = p \cdot 360° \end{cases}$$

$$\begin{cases} (\frac{1}{24} - \frac{1}{88})t = k \\ (\frac{1}{88} - \frac{1}{152})t = p \end{cases}$$

$$\begin{cases} \frac{11-3}{8 \cdot 11 \cdot 3}t = k \\ \frac{19-11}{8 \cdot 11 \cdot 19}t = p \end{cases}$$

$$\begin{cases} t = 3 \cdot 11k \\ t = 11 \cdot 19p \end{cases}$$

che è equivalente a dire che $t$ deve essere un multiplo di $3, 11$ e 19 e quindi un multiplo del loro minimo comune multiplo, ovvero 627. A questo punto è evidente che $s = 627$.
**627**

**Esercizio 16.** Determinare il più piccolo primo $p$ tale che

$$\begin{cases} p^{2222} \equiv p \mod 11 \\ (p-2)^p \equiv 2p \mod 23 \end{cases}$$

Supponiamo che $q$ sia un primo che risolve il precedente sistema. Distinguiamo due casi:

- $q \equiv 0 \mod 11$. Allora banalmente $q = 11$, ma $(11-2)^{11} \equiv 3^{22} \equiv 1 \mod 23$ e non $-1 \mod 23$. Di conseguenza 11 non risolve il sistema di partenza;

- $M.C.D.(11, q) = 1$, ovvero $q \neq 11$. Per ipotesi abbiamo che

$$\begin{cases} q^{2222} \equiv q \mod 11 \\ (q-2)^q \equiv 2q \mod 23 \end{cases}$$

ma $2222 \equiv 2 \mod 10 = \phi(11)$, da cui il precedente sistema è equivalente a

$$\begin{cases} q^{2} \equiv q \mod 11 \\ (q-2)^q \equiv 2q \mod 23 \end{cases}$$

da cui

$$\begin{cases} q \equiv 1 \mod 11 \\ (q-2)^q \equiv 2q \mod 23 \end{cases}$$

Per la prima congruenza non è riduttivo supporre che $q = 11k + 1$. A questo punto ci chiediamo quindi per quali primi $q$ della forma $11k + 1$ vale che $(q-2)^q \equiv 2q \mod 23$. Questa condizione può essere riscritta come $(11k-1)^{11k+1} \equiv 22k+2 \mod 23$. A questo punto notiamo che $11k-1$ non può essere divisibile per 23, in quanto altrimenti lo dovrebbe essere anche $11k + 1$, e quindi $(11k-1)^{11k} \equiv \pm 1 \mod 23$. Questo perché $(11k-1)^{11k}$ è soluzione di $x^2 \equiv 1 \mod 23$ che, per il Lemma di Euclide e la fattorizzazione $x^2 - 1 = (x-1)(x+1)$, implica $x \equiv \pm 1 \mod 23$ (Nota: $\mathbb{Z}/pZ$ è un campo). Perciò deve valere o $11k - 1 \equiv 22k + 2 \mod 23$ o $1 - 11k \equiv 22k + 2 \mod 23$. La prima congruenza è equivalente a $k+2 \equiv 2k-4 \mod 23$ (basta moltiplicare per $-2$ ambo i membri), e quindi $k \equiv 6 \mod 23$, da cui $q \equiv 6 \cdot 11 + 1 = 67 \mod 23 \cdot 11$: il minimo primo siffatto è 67, che è effettivamente soluzione del sistema. La seconda congruenza è equivalente a $k + 2 \equiv -2k + 4 \mod 23$, da cui $3k \equiv 2 \mod 23$ e dunque $k \equiv 16 \mod 23$ e quindi $q \equiv 11 \cdot 16 + 1 \mod 11 \cdot 23$, ovvero $q \equiv 161 \mod 11 \cdot 23$: il minimo intero siffatto è 161, che è maggiore di 67. Perciò $p = 67$.

**67**

**Esercizio 17.** Determinare il minimo intero positivo $x$ tale che $209 | x^{201} - x^{21} + 11x$.

Giacché $209 = 11 \cdot 19$, determiniamo innanzitutto tutte le soluzioni di

$$\begin{cases} y^{201} - y^{21} + 11y \equiv 0 \mod 11 \\ y^{201} - y^{21} + 11y \equiv 0 \mod 19 \end{cases}$$

Poiché $201 \equiv 21 \mod 10 = \phi(11)$ e $201 \equiv 21 \mod 18 = \phi(19)$, risulta che $y^{201} \equiv y^{21}$ sia modulo 11 che modulo 23. Di conseguenza il precedente sistema è equivalente a $11y \equiv 0 \mod 19$, da cui $y \equiv 0 \mod 19$. A questo punto è evidente che $x = 19$.

**19**

**Esercizio 18.** Detti $n = 600!$ e $m = 177! \cdot 313! \cdot 111!$, trovare il resto della divisione tra $n$ e $m$.(Se tale resto fosse maggiore di 9999, indicare come risposta 9999)

Innanzitutto dimostriamo un lemma molto utile: $\lfloor a \rfloor + \lfloor b \rfloor \leq \lfloor a + b \rfloor$. Difatti da $\lfloor a \rfloor \leq a$ e $\lfloor b \rfloor \leq b$ si ottiene $\lfloor a \rfloor + \lfloor b \rfloor \leq a + b$. Ma $\lfloor a \rfloor + \lfloor b \rfloor \in \mathbb{Z}$, da cui $\lfloor a \rfloor + \lfloor b \rfloor \leq \max\{x \in \mathbb{Z} | x \leq a + b\} = \lfloor a + b \rfloor$. Per l'identità di Legendre-De Polignac risulta che $\nu_p(x!) = \sum_{i=1}^{+\infty} \lfloor \frac{x}{p^i} \rfloor$ con $p$ primo e $x$ naturale. Giacché la valutazione $p$-adica è una funzione logaritmica (ovvero $\nu_p(xy) = \nu_p(x) + \nu_p(y)$), allora $\nu_p(m) = \nu_p(177!) + \nu_p(313!) + \nu_p(111!) = \sum_{i=1}^{+\infty} \lfloor \frac{177}{p^i} \rfloor + \sum_{i=1}^{+\infty} \lfloor \frac{313}{p^i} \rfloor + \sum_{i=1}^{+\infty} \lfloor \frac{111}{p^i} \rfloor = \sum_{i=1}^{+\infty} \lfloor \frac{177}{p^i} \rfloor + \lfloor \frac{313}{p^i} \rfloor + \lfloor \frac{111}{p^i} \rfloor \leq \sum_{i=1}^{+\infty} \lfloor \frac{177+313+111}{p^i} \rfloor = \nu_p(601!) = \nu_p(n) + \nu_p(601)$. Siccome 601 è primo, allora per ogni $p \leq 600$ primo risulta che $\nu_p(m) \leq \nu_p(n)$ e quindi $m | n$, da cui $s = 0$.

**0**

**Esercizio 19.** Sull'isola di *Kenoncè* i distributori di caramelle hanno due pulsanti: se si preme il primo pulsante esce un numeri fissato $x$ di caramelle mentre se si preme il secondo ne esce un numero fissato $y$. Leo va con 10 suoi amici, preme 3 volte il primo pulsante e 7 volte il secondo, e poi prova a dividere le caramelle in 11 parti uguali, ma non

ci riesce perché ne restano 9. Arrivano altri due amici , e decidono di premere entrambi i pulsanti altre due volte, sperando che aggiungendo le nuove caramelle a tutto il mucchio precedente si riesca a dividerle in parti uguali tra 13 persone, ma anche questa volta non ci riescono perché gliene restano 2.
Trovare tutte le possibili coppie $(x, y)$ che soddisfano le ulteriori condizioni $0 < x \leq 75$ e $0 < y \leq 100$. Dare come risposta il numero che si ottiene aggiungendo alla somma di tutti i possibili $y$ il doppio della somma di tutti i possibili $x$.

In pratica ci viene detto che

$$\begin{cases} 3x + 5y \equiv 9 \mod 11 \\ 5x + 7y \equiv 2 \mod 13 \end{cases}$$

Poiché $3 \equiv -8 \mod 11, 5 \equiv -8 \mod 13, 5 \equiv -4 \mod 11$ e $7 \equiv -4 \mod 13$, il precedente sistema è equivalente a

$$\begin{cases} -8x - 4y \equiv 9 \mod 11 \\ -8x - 4y \equiv 2 \mod 13 \end{cases}$$

ovvero

$$\begin{cases} 2x + y \equiv -27 \mod 11 \\ 2x + y \equiv 6 \mod 13 \end{cases}$$

che è equivalente a

$$\begin{cases} 2x + y \equiv 6 \mod 11 \\ 2x + y \equiv 6 \mod 13 \end{cases}$$

che a sua volta, per il teorema cinese del resto, è equivalente a $2x + y \equiv 6 \mod 143$. Da $x \leq 75$ e $y \leq 100$ si ottiene che $2x + y \leq 150 + 100 = 250$, da cui $2x + y = 6$ o $2x + y = 149$. La prima equazione ha esattamente 2 soluzioni come quelle richieste dal problema, mentre la seconda ne ha 50, da cui $s = 2 \cdot 6 + 50 \cdot 149 = 7462$.
**7462**

**Esercizio 20.** Un grillo salta tra i punti a coordinate intere del piano cartesiano. Parte da $(0, 0)$ e vuole arrivare in $(1, 1)$. Ogni salto consiste nel sommare o sottrarre alla sua posizione uno dei seguenti vettori: $(21, 33), (15, 21)$ o $(35, 77)$. Qual è il minimo numero di salti che deve fare?

Cerchiamo prima tutte le soluzioni del sistema

$$\begin{cases} 21x + 15y + 35z = 1 \\ 33x + 21y + 77z = 1 \end{cases}$$

Sottraiamo la prima equazione alla seconda. Otteniamo così il sistema equivalente

$$\begin{cases} 21x + 15y + 35z = 1 \\ 12x + 6y + 42z = 0 \end{cases}$$

ovvero

$$\begin{cases} 21x + 15y + 35z = 1 \\ 2x + y + 7z = 0 \end{cases}$$

A questo punto esplicitiamo $y$ in funzione di $x$ e $z$ e sostituiamo nella prima equazione, ottenendo il sistema

$$\begin{cases} 9x + 70z = -1 \\ y = -2x - 7z \end{cases}$$

Risolvendo la prima equazione si ottiene che $x = 31 + 70k, z = -4 - 9k, y = -34 - 77k$. A questo punto è abbastanza semplice da notare che la soluzione che minimizza la somma dei valori assoluti di $x, y$ e $z$ è $(31, -34, -4)$, da cui $s = 69$.
**69**

**Esercizio 21.** Sia $\phi$ la funzione "*$\phi$ di Eulero*", ovvero $\phi(n)$ indica quanti sono gli interi compresi fra 1 e $n$ che sono coprimi con $n$. Per ogni intero positivo $n$ definiamo

$$a_n = \phi^n(517^{100})$$

dove l'esponente di $\phi$ è considerato rispetto all'operazione di composizione di funzioni. Qual è il più piccolo valore di $n$ per il quale si ha $a_n = 1$.

Innanzitutto notiamo che $517 = 47 \cdot 11$, e quindi $517^{100} = 47^{100} \cdot 11^{100}$. Computiamo $a_1$:

$$a_1 = \phi(47^{100} \cdot 11^{100}) = \phi(47^{100}) \cdot \phi(11^{100}) = 47^{99} \cdot 46 \cdot 11^{99} \cdot 10 = 2^2 \cdot 5 \cdot 11^{99} \cdot 23 \cdot 47^{99}$$

Siano $\{\alpha_i\}_{i \in \mathbb{N}^*}, \{\beta_i\}_{i \in \mathbb{N}^*}, \{\gamma_i\}_{i \in \mathbb{N}^*}, \{\delta_i\}_{i \in \mathbb{N}^*}$ e $\{\varepsilon_i\}_{i \in \mathbb{N}^*}$ le successioni delle valutazioni $2, 5, 11, 23, 47$ -adiche (rispettivamente) degli $a_i$. Supponiamo ora che $a_n = 2^{\alpha_n} \cdot 5^{\beta_n} \cdot 11^{\gamma_n} \cdot 23^{\delta_n} \cdot 47^{\varepsilon_n}$ con $\alpha_n, \beta_n, \gamma_n, \delta_n$ e $\varepsilon_n$ tutti positivi. Allora $a_{n+1} = 2^{\alpha_n - 1} \cdot 2^2 \cdot 5^{\beta_n - 1} \cdot 10 \cdot 11^{\gamma_n - 1} \cdot 22 \cdot 23^{\delta_n - 1} \cdot 46 \cdot 47^{\varepsilon_n - 1} = 2^{\alpha_n + 4} \cdot 5^{\beta_n} \cdot 11^{\gamma_n} \cdot 23^{\delta_n} \cdot 47^{\varepsilon_n - 1}$ e quindi $(\alpha_{n+1}, \beta_{n+1}, \gamma_{n+1}, \delta_{n+1}, \varepsilon_{n+1}) = (\alpha_n + 4, \beta_n, \gamma_n, \delta_n, \varepsilon_n - 1)$. A questo punto è evidente che $a_{100} = 2^{2+99 \cdot 4} \cdot 5 \cdot 11^{99} \cdot 23 = 2^{398} \cdot 5 \cdot 11^{99} \cdot 23$. Computiamo ora $a_{101}$.

$$a_{101} = \phi(a_{100}) = \phi(2^{398} \cdot 5 \cdot 11^{99} \cdot 23) = 2^{397} \cdot 4 \cdot 10 \cdot^{98} \cdot 22 = 2^{401} \cdot 5 \cdot 11^{98}$$

Supponiamo ora che $a_n = 2^{\alpha_n} \cdot 5^{\beta_n} \cdot 11^{\gamma_n}$ con $\alpha_n, \beta_n$ e $\gamma_n$ positivi. Allora $a_{n+1} = \phi(a_n) = 2^{\alpha_{n-1}} \cdot 4 \cdot 5^{\beta_n - 1} \cdot 10 \cdot 11^{\gamma_n - 1} = 2^{\alpha_n + 2} \cdot 5^{\beta_n} \cdot 11^{\gamma_n - 1}$, da cui $(\alpha_{n+1}, \beta_{n+1}, \gamma_{n+1}) = (\alpha_n + 2, \beta_n, \gamma_n - 1)$. A questo punto non è difficile notare che $a_{200} = 2^{401+2 \cdot 99} \cdot 5 = 2^{599} \cdot 5$. Perciò $a_{201} = 2^{600}$ e quindi $a_{801}$ è il primo termine della successione degli $a_i$ pari a 1.
**801**

**Esercizio 22.** Trovare le ultime 4 cifre del numero

$$2^{3^{5^{7^{11^{17^{\cdot^{\cdot^{\cdot^{97}}}}}}}}}$$

dove sono stati usati tutti e soli i numeri primi minori di 100.

Poiché $s$ è il resto dalla divisione di $2^{3^{5^{7^{11^{17^{\cdot^{\cdot^{\cdot^{97}}}}}}}}}$ per 10000, per il teorema cinese del resto è lecito scrivere che tale condizione è equivalente a

$$\begin{cases} s \equiv 2^{3^{5^{7^{11^{17^{\cdot^{\cdot^{\cdot^{97}}}}}}}}} & \mod 2^4 \\ s \equiv 2^{3^{5^{7^{11^{17^{\cdot^{\cdot^{\cdot^{97}}}}}}}}} & \mod 5^4 \end{cases}$$

A questo punto la prima congruenza si può semplificare facilmente, mentre la seconda scritta così è piuttosto ostica.

Per semplificarci la vita, calcoliamo il resto $x$ di $3^{5^{7^{11^{17^{\cdot^{\cdot^{\cdot^{97}}}}}}}}$ dalla divisione per $\phi(5^4) = 4 \cdot 5^3$, che per il teorema cinese del resto si può trovare risolvendo

$$\begin{cases} x \equiv 3^{5^{7^{11^{17^{\cdot^{\cdot^{\cdot^{97}}}}}}}} & \mod 4 \\ x \equiv 3^{5^{7^{11^{17^{\cdot^{\cdot^{\cdot^{97}}}}}}}} & \mod 5^3 \end{cases}$$

Di nuovo la prima congruenza è molto semplice, ma la seconda per niente. Per questo motivo, onde semplificarci i conti, calcoliamo il resto $y$ di $5^{7^{11^{17^{\cdot^{\cdot^{\cdot^{97}}}}}}}$ dalla divisione per $\phi(5^3) = 4 \cdot 5^2$. Sempre per il teorema cinese del resto possiamo scrivere che

$$\begin{cases} y \equiv 5^{7^{11^{17^{\cdot^{\cdot^{\cdot^{97}}}}}}} & \mod 4 \\ y \equiv 5^{7^{11^{17^{\cdot^{\cdot^{\cdot^{97}}}}}}} & \mod 5^2 \end{cases}$$

che è banalmente equivalente a

$$\begin{cases} y \equiv 1 \mod 4 \\ y \equiv 0 \mod 5^2 \end{cases}$$

e quindi $y = 25$. A questo punto possiamo riscrivere il sistema

$$\begin{cases} x \equiv 3^{5^{7^{11^{17^{\cdot^{\cdot^{\cdot^{97}}}}}}}} \mod 4 \\ x \equiv 3^{5^{7^{11^{17^{\cdot^{\cdot^{\cdot^{97}}}}}}}} \mod 5^3 \end{cases}$$

come

$$\begin{cases} x \equiv -1 \mod 4 \\ x \equiv 3^{25} \mod 5^3 \end{cases}$$

A questo punto, per fare i conti, potrebbe essere conveniente sfruttare il fatto che $3^5 = 243 \equiv -7 \mod 5^3$, ottenendo

$$\begin{cases} x \equiv -1 \mod 4 \\ x \equiv 68 \mod 5^3 \end{cases}$$

e dunque $y = 443$. A questo punto possiamo riscrivere il sistema iniziale come

$$\begin{cases} s \equiv 0 \mod 2^4 \\ s \equiv 2^{443} \mod 5^4 \end{cases}$$

L'espediente con cui adesso ci liberiamo di moltissimi calcoli è quello di scrivere $2^{443}$ come $2 \cdot (2^2)^{221} = 2 \cdot (5-1)^{221} \equiv 2 \cdot ((-1)^{221} + \binom{221}{1}(-1)^{220} \cdot 5 + \binom{221}{2}(-1)^{219} \cdot 5^2 + \binom{221}{3}(-1)^{218} \cdot 5^3) \equiv 2 \cdot [-1 + 5 \cdot (-29) - 5^2 \cdot 10] \equiv 2 \cdot (-396) \equiv 458 \mod 625$. Perciò il precedente sistema può essere riscritto come

$$\begin{cases} s \equiv 0 \mod 2^4 \\ s \equiv 458 \mod 5^4 \end{cases}$$

e dunque, con i soliti metodi di risoluzione di questi sistemi, si ottiene che $s = 4208$.
**4208**

**Esercizio 23.** Trovare tutti gli $n$ interi positivi tali che $\phi(n) = 60$, dove $\phi$ è la cosiddetta funzione "$\phi$ *di Eulero*", ovvero $\phi(n)$ indica quanti sono gli interi compresi tra 1 e $n$ che sono coprimi con $n$.

Supponiamo quindi che $\phi(n) = 60 = 2^2 \cdot 3 \cdot 5$. Una conseguenza della moltiplicatività della funzione di Eulero è che se $p$ primo divide $n$ allora $p-1$ divide $\phi(n)$. Siccome tutti e i soli primi che si ottengono sommando 1 ad un divisore di 60 sono $2, 3, 5, 7, 11, 13, 31, 61$, abbiamo che $n = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \cdot 11^e \cdot 13^f \cdot 31^g \cdot 61^h$. Se $61|n$ allora $h = 1$ e $\phi(\frac{n}{61}) = 1$, da cui $n = 61$ o $n = 2 \cdot 61$. Supponiamo ora che 61 non divide $n$. Se $31|n$ allora $g = 1$ e quindi $\phi(\frac{n}{31}) = 2$, da cui $n = 3 \cdot 31$ o $n = 4 \cdot 31$ o $n = 6 \cdot 31$. Supponiamo ora che 31 non divide $n$. Se $11|n$ allora $f = 1$ e $\phi(\frac{n}{11}) = 6$, da cui $n = 11 \cdot 7$ o $n = 11 \cdot 7 \cdot 2$ o $n = 11 \cdot 9$ o ancora $n = 11 \cdot 9 \cdot 2$. Supponiamo ora che 11 non divide $n$. Se $7|n$ allora $d = 1$ e $\phi(\frac{n}{7}) = 10$, e si ottengono così unicamente soluzioni già considerate. Supponiamo ora che 7 non divide $n$. Se $5|n$ allora $4|\phi(5^c)$ e quindi $\phi(\frac{n}{5^c})$ è dispari e maggiore di 1, contrariamente al fatto che l'unico valore dispari assunto dalla $\phi$ è 1, da cui 5 non divide $n$. Siccome 5 non è un divisore di $\phi(2^a \cdot 3^b)$, necessariamente $s = 61 + 61 \cdot 2 + 31 \cdot 3 + 31 \cdot 4 + 31 \cdot 6 + 11 \cdot 7 + 11 \cdot 7 \cdot 2 + 9 \cdot 11 + 9 \cdot 11 \cdot 2 = 1114$.
**1114**

**Esercizio 24.** Posto $A = 2019!$ indichiamo con $n$ il numero di 0 finali di $A$ e con $c$ la cifra delle unità del numero che si ottiene cancellando da $A$ tutti gli 0 finali. Quanto vale $1000c + n$.

Poiché i fattori 2 che dividono $A$ sono considervolmente di più rispetto ai fattori 5 che dividono $A$, risulta quindi che $n = \lfloor \frac{2019}{5} \rfloor + \lfloor \frac{2019}{25} \rfloor + \lfloor \frac{2019}{125} \rfloor + \lfloor \frac{2019}{625} \rfloor = 403 + 80 + 16 + 3 = 502$. Sia $B = \frac{A}{10^{502}}$. Allora vale che

$$\begin{cases} B \equiv c \mod 2 \\ B \equiv c \mod 5 \end{cases}$$

Poiché $2|B$ si ha che $c \equiv 0 \mod 2$. Notiamo che la seconda congruenza può essere riscritta come $c \equiv -\frac{A}{5^{502}} \mod 5$. Denotiamo ora con $\overline{i} = \{x \in \mathbb{N}^* : 5^i | x \wedge 5^{i+1} \not| x\}$ e sia $f$ la funzione che associa, insieme per insieme, i numeri $1, 2, 3$ e 4 ciclicamente. Ad esempio $f$ associa a $1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16 \dots$ i numeri $1, 2, 3, 4, 1, 2, 3, 4, 1, 2, 3, 4, 1, \dots$, a $5, 10, 15, 20, 30, 35, 40, 45, 55, 60, 65, 70, 80, \dots$ i numeri $1, 2, 3, 4, 1, 2, 3, 4, 1, 2, 3, 4, 1 \dots$ e così via per gli altri insiemi. Dimostriamo che $\frac{A}{5^{402}} \equiv \prod_{i=1}^{2019} f(i)$. Per farlo dimostriamo che per ogni $n$ naturale vale che $\frac{n}{5^{\nu_5(n)}} \equiv f(n) \mod 5$, e lo dimostriamo per induzione sugli insiemi $\overline{i}$:

- se $i = 0$ allora l'asserzione da dimostrare è banale (per una dimostrazione formale di questo fatto piuttosto ovvio, basterebbe far vedere che la cosa vale per $1, 2, 3, 4$ e poi si fa vedere che $p(n) \Rightarrow p(n+5)$);
- supponiamo che la proprietà valga per gli elementi di $\overline{i}$ e dimostriamola per gli elementi di $\overline{i+1}$. Si vede facilmente (e si dimostra formalmente per induzione) che preso un elemento $x$ di $\overline{i}$ e associatogli $5x$ in $\overline{i+1}$ (tale associazione è ovviamente una funzione bigettiva da $\overline{i}$ in $\overline{i+1}$) si ha che $f(x) = f(5x)$, e quindi si conclude sfruttando il fatto che $\frac{5x}{5^{\nu_5(5x)}} = \frac{x}{5^{\nu_5(x)}} \equiv f(x) \equiv f(5x) \mod 5$ e quindi il claim è dimostrato per induzione forte.

Poiché in $[1, 2019]$ abbiamo $2019 - 403 = 1616$ elementi di $\overline{0}$, $403 - 80 = 323$ elementi in $\overline{1}$, $80 - 16 = 64$ elementi in $\overline{2}$, $16 - 3 = 13$ elementi in $\overline{3}$ e 3 elementi in $\overline{4}$, evidentemente $c \equiv -\frac{A}{5^{402}} \equiv -(1 \cdot 2 \cdot 3 \cdot 4)^{\frac{1616}{4} + \frac{320}{4} + \frac{64}{4} + \frac{12}{4}} \cdot (1 \cdot 2 \cdot 3)^2 \equiv 1 \mod 5$ e dunque $c = 6$. Perciò $s = 6502$.

**6502**