IN QUANTO TEMPO SI PUÒ CALCOLARE LA CIFRA DELLE UNITÀ DI 1173^{219}?

1. Introduzione.

Notando che tanto 1173 quanto 219 sono due numeri scelti del tutto a caso, si può rispondere in generale che, dati una base e una potenza qualsiasi, in quattro casi su dieci la risposta è immediata (dipende dai riflessi di chi risponde, quindi tra 0.3 secondi e un secondo) e negli altri casi può essere data in meno di un minuto.

In realtà, questo curioso risultato mi è venuto in mente provando a rispondere alla seguente domanda comparsa su Quora (in inglese):

Qual è la cifra delle unità di 3^{100} (utilizzando il teorema di Fermat?)

Così come è formulata su Quora, la domanda richiede la conoscenza del (Piccolo) Teorema di Fermat. Ci sono quindi due classi di lettori:

(1) quelli che non conoscono il Piccolo Teorema di Fermat o PTF (ovviamente da non confondersi con il Teorema di Fermat per eccellenza, recentemente dimostrato da A. Wiles (1994), che afferma che ***non esistono quattro numeri naturali , o interi maggiori di 0, m, n, h, k, tali che*** $m^h + n^h = k^h$ ***per*** $h > 2$). Questa classe di lettori, evidentemente non può cimentarsi con il problema così come è formulato, a meno di impararsi il Piccolo Teorema di Fermat, la cui dimostrazioe è del resto reperibile ovunque. I pigri la possono trovare spiegata altrove in questo sito (Il Piccolo Gigante - piccolo teorema di Fermat (dainoequinoziale.it))

(2) Quelli che conoscono il Piccolo Teorema di Fermat, e quindi sono invitati a trovare il modo di applicare una formula nota. Questo teorema cade per loro (quasi del tutto) nella classe dei problemi meno istruttivi, che consistono nell'applicazione di un paio di formule, anche complicate, ma note, senza scomodare troppo la materia grigia che occupa la scatola cranica, con un'operazione in pratica di pura memoria.

In questo saggio cercherò di risolvere il problema come richiesto in tre modi, applicando anche un'estensione del PTF, dovuta ad Euler, che dà immediatamente la soluzione – naturalmente purché si conosca questo teorema di Euler, che a sua volta implica la conoscenza della sua funzione "ϕ" (sulla quale scrivo qualcosa in questo sito: La funzione Phi di Euler (dainoequinoziale.it)).

La parte fastidiosa della risposta alla domanda comparsa su Quora è come trascinare l'inutile (piccolo) teorema di Fermat nella soluzione del problema. Inoltre, utilizzando il PTF e derivati non si ha in mano un metodo veloce di ottenere il risultato e sue estensioni. **Sarà quindi (forse) sorprendente scoprire che usando metodi elementari, si troverà rapidamente assai di più di quanto richiesto da Quora.**

2. Prima Soluzione con il Piccolo Teorema di Fermat (PTF).

Riporto la soluzione di *Mohammad Afzaal Butt*, approvata da Math Central, sito specializzato di Quora (in inglese). Scrivo in nero il testo originale, in rosso i miei commenti.

La cifra dell'unità è il resto di 3^{100} diviso per 10.
$10 = 2\times5$
$3 \equiv 1 \pmod 2$ *(questo lo si trova direttamente dividendo 3 per 2, o anche applicando una prima volta il PTF, che afferma che* ***$a^{p-1} \equiv 1 \pmod p$*** *per a, p primi fra loro o co-primi. In altre parole, l'espressione $(a^{p-1} - 1)$ è divisibile per p. Ora, inserendo nella formula del PTF a = 3 e p=2, che sono primi fra loro, si trova appunto $3^1 = 1 \pmod 2$)*

Con un minimo di ragionamento, o applicando una opportuna proprietà (che chiameremo Proprietà I delle congruenze, che in forma sintetica afferma che "il resto (ovvero, brevemente , "la congruenza") di un prodotto è dato dal prodotto dei resti (ovvero "delle congruenze")), si ottiene: 3 x 3 x 3 x 3 …. ≡ 1 x 1 x 1 x1 x 1…(mod 2), che porta a :

(i) ***$\Longrightarrow 3^{100} \equiv 1 \pmod 2$*** *(altro modo di scrivere che $3^{100} = 1 + 2M$) dove M è un intero opportuno.*

Ora l'autore della soluzione afferma che

(3 , 5) = 1. *Nella nostra notazione diremmo che MCD (3,5) = 1, cioè che 3 e 5 sono primi fra loro.*

Quindi per il piccolo teorema di Fermat *(infatti, poiché 3 e 5 sono primi fra loro, si può applicare direttamente il PTF, $a^{p-1} \equiv 1 \pmod p$, che nel nostro caso diventa):*

$3^4 \equiv 1 \pmod 5$ *(cioè $3^4 = 1 + 5N$), dove N è un intero opportuno.*

(ii) ***$\Longrightarrow 3^{100} \equiv 1 \pmod 5$*** *(Questo perché 100 = 4 * 25, e a $(3^4)^{25}$ si può applicare la Proprietà I, citata più sopra.)*

Inoltre
(2 , 5) = 1.
Quindi per (i) e (ii)

(iii) ***$3^{100} \equiv 1 \pmod{2\times5}$***
$\Longrightarrow 3^{100} \equiv 1 \pmod{10}$

Quindi la cifra dell'unità (di 3^{100}) è 1.

Il risultato è corretto, e la dimostrazione elegante, ma a me pare che la (iii) richieda qualche spiegazione. In effetti si tratta di una proprietà che normalmente viene dimostrata a parte dalle altre proprietà delle conguenze. Tuttavia, nel caso presente, possiamo facilmente scrivere:

$3^{100} - 1 = 2M$

$3^{100} - 1 = 5N$,

sottraendo membro a membro abbiamo: $0 = 2M-5N$, che si risolve in generale ponendo $M = 5k$ e $N= 2k$, vale a a dire:

$3^{100} - 1 = 10k$ per entrambi i moduli, 2 e 5, che è solo un altro modo di scrivere che $3^{100} \equiv 1 \pmod{2 \times 5 = 10}$.

> Perché l'autore sottolinea che il MCD di 2 e 5 è eguale a 1, cioè che i numeri sono primi fra loro? Nella dimostrazione da me data , questo non è necessario, ma qui probabilmente l'autore ha in mente un altro teorema, il teorema cinese del resto (TCR), che afferma che "per qualsiasi a e b, e due co-primi m, n esiste un unico x (mod mn) tale che $x \equiv a \pmod{m}$ e $x \equiv b \pmod{n}$." La soluzione generale dunque richiede che m e n siano appunto primi fra loro. Noi abbiamo aggirato la non banalissima dimostrazione partendo dalla soluzione a noi nota del nostro caso particolare. Incidentalmente, il più piccolo numero $x \pmod{10}$ tale che $x \equiv 1 \pmod{2}$ e $x \equiv 1 \pmod{5}$ è 81, che, come si può verificare, è un divisore di 3^{100}.

3. Variazioni sul tema del PTF.

La domanda a questo punto è: "Si può semplificare questa dimostrazione?". E la risposta è che esistono almeno due modi.

3.1 Variazione I sul tema del PTF

Il Piccolo Teorema afferma che, dati due co-primi a e p, a^{p-1} / p dà 1 come resto. Selezioniamo quindi a = 3, b = 5 (co-primi), e abbiamo che $3^{(5-1)} = 3^4 = 81$, che, diviso 5, dà resto = 1, come previsto, e come appena notato.

Applichiamo ora la proprietà già utilizzata che sinteticamente afferma che "Il resto del prodotto è eguale al prodotto delle dei resti". Supponiamo $a_i = 3^4$, e n = 5: allora abbiamo $a_1 a_2 = 3^4 3^4 \cdots \equiv 1 \times 1 \pmod{5}$, ed aggiungendo fattori 3^4 a piacere continuiamo ad avere 1 (mod 5).

In conclusione, $3^{4m} = 1 \pmod{5}$, per qualsiasi valore di m.

Fin qui abbiamo seguito più o meno pedissequamente la dimostrazione precedente.

A questo punto, invece di applicare automaticamente la proprietà del prodotto dei moduli, ragioniamo un poco: il fatto che una divisione Q/5 dia resto = 1 significa che **Q termina con 6 o con 1**, come si vede calcolando Q = 1+ 5m, per i primi valori di m.

Ma nessuna potenza di 3 ha 6 come cifra delle unità, perché tutte le potenze dei numeri dispari sono dispari (*), e quindi l'unica possibilità è che 3^{4m} abbia, come cifra delle unità, 1. Essendo 100 un multiplo di 4, il resto della divisione di 3^{100} per 5 è 1, e la cifra delle unità di 3^{100} è 1.

3.2 Variazione II sul tema del PTF

Se fosse permesso andare più veloci, si userebbe un sottoprodotto del Piccolo Teorema, dovuto, inevitabilmente, a Eulero, che afferma che:

"Se a e n sono numeri naturali coprimi, allora $a^{\phi(n)} \equiv 1 \pmod n$, dove ϕ è la funzione Phi di Eulero." Ovviamente bisogna sapere che cosa è la funzione ϕ di Eulero e almeno il valore di $\phi(10)$, che è 4 (**)

La dimostrazione di questo teorema la si può avere con mezzi elementari (si veda https://it.wikipedia.org/wiki/Teorema_di_Eulero_(aritmetica_modulare)).

> L'attento lettore vedrà subito che se *n* è un numero primo *p*, allora $\phi(p) = p-1$, che ci restituisce il PTF. Infatti, la definizione della $\phi(n)$ è che essa è il numero di tutti i numeri tra 1 e n (incluso 1) che sono primi con n. Si noti la presenza di 1, che divide tutti i numeri, ma è coprimo con tutti i numeri, perché la definizione di due numeri coprimi è che il loro MCD sia 1, ciò che è sempre il caso con 1.

Ora applichiamo il teorema di Euler per n = 10, sapendo che $\phi(10) = 4$, e, per a = 3 (primo rispetto a 10) otteniamo che $3^4/10$ dà come resto 1, cioè la cifra unità di 3^4. Sappiamo infatti che $3^4 = 81$. Applichiamo nuovamente la proprietà I del "prodotto delle congruenze" e, poiché 100 è un multiplo di 4, deduciamo che la cifra unità di 3^{100} è 1.

4. Tuttavia…

Le due soluzioni sopra riportate sono probabilmente le vie più astruse, più ottuse e meno stimolanti per ottenere il nostro risultato, in quanto si tratta, specialmente nel secondo caso, di automatiche applicazioni di formule che si suppongono note. Inoltre non permettono certo di trovare una soluzione rapida per il caso da me scelto $\mathbf{1173^{219}}$.

Ma si può ottenere molto di più con molto meno.

La seguente tabella delle potenze dei numeri da 1 a 10 consente alcune interessanti, seppur elementari, considerazioni:

esponente	1	2	3	4	5	6
1	1	1	1	1	1	1
2	2	4	8	16	32	64
3	3	9	27	81	243	729
4	4	16	64	256	1024	4096
5	5	25	125	625	3125	15625
6	6	36	216	1296	7776	46656
7	7	49	343	2401	16807	117649
8	8	64	512	4096	32768	262144
9	9	71	729	6561	59049	531441

Tav.I

Su fondo giallo sono scritti i numeri dispari.
(Noto che la tavola non contiene le potenze di 0, caso anche più banale di quello di 1)

Anzitutto, come dimostrato in nota (*) qualsiasi potenza di una base pari è un numero pari; qualsiasi potenza di una base dispari è un numero dispari. (Ricordo che questo spiega perché abbiamo escluso la cifra delle unità 6 dalle possibilità per 3^{100}.)

In secondo luogo, vediamo che la tavola richiede dei calcoli abbastanza lunghi, ma non necessari. Questo è perché noi conserviamo tutte le cifre dei nostri risultati per le potenze successive. Ma evidentemente la tavola può essere semplificata, perché nel fare il prodotto di due numeri, non importa di quante cifre, la cifra delle unità è inevitabilmente la cifra delle unità del prodotto delle cifre delle unità dei due numeri. Ad esempio si vede subito, eseguendo il prodotto, che l'ultima cifra di 24 x 66 (= 1584) è 4, che è l'ultima cifra di 4 x 6 = 24.

In Tavola I, quindi, le cifre delle unità (segnate in colore) non valgono soltanto per le potenze dei numeri di una cifra, ma valgono per le potenze di tutti i numeri, perché è solo la cifra finale quella che conta. Quindi, se eleviamo, ad esempio, 11243 alle prime sei potenze, le cifre delle unità saranno sempre 3,9,7,1,3,9,… le stesse delle prime sei potenze di 3, incuranti dell'esistenza di quattro cifre (in questo caso 1124) prima della finale 3.

Guardiamo ancor meglio la Tavola I.

Quando da una potenza con base b (con cifra delle unità k), e esponente n, che per noi sarà b^n, passiamo alla successiva , $b^{n+1} = b^n \times b$, necessariamente le cifre delle unità si susseguono in cicli di quattro. In effetti, l'ultima cifra della base essendo fissa (le abbiamo dato nome ***k***), ogni volta che una cifra delle unità ***m*** di b^n compare, la cifra delle unità della potenza successiva sarà sempre data dall'ultima cifra del prodotto di ***m*** per ***k***. Non solo, ma si ripresenteranno in ordine anche le cifre delle unità delle

potenze successive. Osserviamo ancora che dobbiamo considerare solo quattro numeri dispari (escluso il 5, al quale non si può arrivare in altro modo che moltiplicando numeri che terminano per 5) e quattro numeri pari. Pertanto, le cifre hanno al massimo un ciclo di lunghezza quattro, oppure un divisore di quattro. Questo lo si vede anche dalla Tav.I, da cui appare che **1, 5 e 6** hanno un ciclo di lunghezza 1; **9** ha un ciclo di lunghezza 2; **3,4, 7,8** hanno un ciclo di lunghezza 4. Ne segue che l'ultima cifra di qualsiasi potenza di qualsiasi numero che termina con 1, 5, 6 è ancora 1,5,6. Poiché lo stesso vale per 0, come si vede subito banalmente (non abbiam fatto allo zero neppure l'onore di includerlo nella Tavola I), in 4 casi su dieci, per basi che terminano con le cifre 0,1,5,6, sappiamo subito la cifra finale di qualsiasi potenza, che sarà ancora 0, 1, 5, 6.

Inoltre, data come cifra delle unità di un numero qualsiasi una qualunque delle nove cifre, k (incluso il caso dello zero, che è davvero banale), poiché il ciclo ha lunghezza 4 o un suo divisore, la quinta potenza deve essere tale da permettere di ricominciare il ciclo, cioè la cifra delle unità della quinta potenza deve essere la cifra iniziale k (***). Ma, se la cifra delle unità della quinta potenza è k, che è il prodotto di k per la cifra delle unità di b^4, allora tutti i numeri dispari devono presentare 1 come cifra delle unità della quarta potenza e delle potenze che hanno come esponente un multiplo di 4. Ciò non è possibile per k pari, perché tutte le potenze di numeri pari sono numeri pari e quindi non possono terminare con 1. Esiste però (fatto poco noto) un numero pari compreso fra 0 e 9, che , moltiplicato per qualsiasi numero pari, riproduce la cifra delle unità di tale numero. Si può provare a scoprirlo, e si troverà che, chissà perché, il numero è 6, e infatti abbiamo 6 x 2 = 12; 6 x 4 = 24; 6 x 6 = 36; 6 x 8 = 48.

Quindi, eccetto 5, tutti i numeri dispari (1,3,7,9) presentano una cifra delle unità eguale a 1 in tutte le potenze i cui esponenti sono multipli di 4, mentre tutti i numeri pari (2,4,6,8) presentano una cifra delle unità eguale a 6 in tutte le potenze i cui esponenti sono multipli di 4. Già a questo punto possiamo concludere che non solo 3^{100}, ma anche 17^{100} e 133^{144} hanno 1 come cifra delle unità.

Infatti:

3^{100} = 515377520732011331036461129765621272702107522001

17^{100} =
1108899372780783641306111715875094966436017167649879524402769841278887580501366697712424694256005093589248451503068397608001

133^{144} =
6833391439274809250328106443530507037637728600529706965565978026606549926563786764115576691778138458495501765414348891531584003590974614251523416960795146093093882957359836671182793674651041192949205483212207741848390383428552478428128469534815794984085917238822483376587650515970729439016196353094009379211

E infine 122^{100} ha una cifra finale 6.

122^{100} =
43249696826361043810151245715112711473319706363607432487649394522053394366515996692882709029518204794420792096166151949884473826116159074978429835068670400966710494153905063879417047163087382303770706890981 37 .

Usando Tavola I con criterio, possiamo dedurre in breve tempo l'ultima cifra di qualsiasi potenza di qualsiasi numero, non solo di 3^{100}, utilizzando soltanto nozioni di aritmetica elementare (nessuna congruenza, nessun Piccolo Teorema di Fermat o di Eulero).

L'unico problema che non ho ancora affrontato, è quello di identificare se l'esponente, che può avere anche 40 cifre, è della forma 4N, 4N+1, 4N+2, 4N+3. Per questo esiste una semplice regola. Si prende il numero formato dalle ultime due cifre dell'esponente (o di qualsiasi numero) e lo si divide per 4. Se il resto della divisione è 0, il numero è della forma 4N, cioè è divisibile per quattro. Se il resto è ***h*** (= 1, 2, 3), il numero è della forma 4N+h. Come lo si dimostra? Come è noto, un numero in base decimale della forma ***abcd = 1000*a+ 100*b+ 10 *c + d.*** Ora, 10/4 dà resto 2 e tutte le altre potenze di 10 danno resto 0. Applicando due note proprietà delle congruenze, che sinteticamente possono essere enunciate come "il resto della somma è la somma dei resti; il resto del prodotto è il prodotto dei resti", vediamo che il resto di (1000*a+ 100*b+ 10 *c + d)/4 è eguale al resto di (10*c +d)/4, cioè al resto del numero formato dalle due ultime cifre divso 4.

A questo punto, si può fare meglio compilando una "tavola ridotta" (Tavola II) basandoci sui fatti che abbiamo notato.

k \ n	n = 4N +1	n = 4N+2	n= 4N+3	n=4(N+1)
0	0	0	0	0
1	1	1	1	1
2	2	4	8	6
3	3	9	7	1
4	4	6	4	6
5	5	5	5	5
6	6	6	6	6
7	7	9	3	1
8	8	4	2	6
9	9	1	9	1

Tav. II

Cifre delle unità delle potenze b^n. In prima colonna, la cifra delle unità k della base b. N è un numero qualsiasi.Si può vedere che la colonna n = 4N+1 riproduce k.

La tavola è interessante, e la lascio allo studio di chi crede. Ma supponiamo che vi si chieda quanto fa 138^{221}. Si costruisce in pochi secondi la riga di k= 8: **8**, 8 x 8 =64, tengo **4**; 8x 4 =32, tengo **2**; 8 x 2 = 16, tengo **6, dopodiché si ricomincia da capo.** Ma per conoscere il resto della divisione di 221 per 4, basta il resto della divisione per 4 del numero formato dalle **due ultime cifre**. Deduciamo quindi che 221 è del tipo 4N+1. E si vede che, diversamente da come abbiamo fatto a scopo dimostrativo, conviene calcolare per prima cosa il resto della divisione per quattro dell'esponente, perché in questo caso ci saremmo risparmiati la fatica di calcolare l'intera riga 8. Quindi la cifra delle unità della nostra potenza è 8. Il risultato è infatti

818989048968437965825969106892104656309996460160407052531214918700378352665837444929284697857545366159051363575777902952406980587480220125660551659124364646482008139845707814772451979173569436247021139809853395647342673405989435423720195350399518460710059249847351372219245831638484515266521940319829525542278836153084953325123987875435790032688796470956917751661308977218087373126582155169352118996663132701842444472921429563255724541849036465080639825308729900402611322288

Supponiamo di volere la cifra delle unità di 1173^{219}. Non importa quanto grande possa essere il risultato, il resto della divisione per 4 di 219 è il resto di 19 /4, che vale 3, e quindi la cifra delle unità sarà 7. In effetti, come può essere subito dimostrato da qualsiasi programma specializzato, 1173^{219} =

=150059900207572452870777839962843384198983400088091203888982239513910083617711827722191500704059016479620497489850835522557345072863018001037725724577048026042262271496257226859106871911177112108338567092696391482261459663360586736903427204307371007373124774526663971442366463016630761474647731403879860815557931752635278767181351158294116150923337833269273305228077159669914167246993708144113568731536972837097990191730918533789899517190134019875653678188489164270964955229957537802848807692069194924589588317641957968917910042449030739220475324153630069181978260237989844896672207387365947108926441627509257801502343583685801262737233205463102114637633634905006195682637

Peccato che il nostro metodo ci dia solo l'ultima cifra!

In conclusione, occorre meno di un minuto per calcolare la cifra delle unità di qualsiasi numero (anche di 1000 cifre) espresso in notazione decimale elevato a qualsiasi esponente (anche di 1000 cifre). Nel caso di 3^{100} si calcola il resto della divisione 100/4, che è zero; e quindi 3, 9, 27, 81, che ci dà 1 come cifra finale.

Problemi affini.

Su questa base si possono rapidamente risolvere problemi affini. Per esempio:

"Qual è la cifra delle unità della somma $1+ 2^{100} + 3^{100}$? Risposta, 8. "

"Qual è la cifra delle unità del prodotto $1 \times 2^{100} \times 3^{100}$? Risposta, 6. "

"Qual è la cifra delle unità dell'espressione $11^{1983}+17^{1983}-7^{1983}$? Risposta, 1. "

Si noti che numeri che terminano con la stessa cifra, per diversi che siano, elevati alla stessa potenza hanno eguali cifre delle unità.

NOTE

(*) Questo lo si vede subito notando che il prodotto di due numeri pari (cioè della forma 2n) è un numero pari e il prodotto di due numeri dispari (cioè della forma 2n+1) è un numero dispari. In effetti 2n *2m = 4mn = 2 (2mn) = 2M; mentre (2m+1)(2n+1) = 4mn + 2m +2n +1= 2(2mn+m+n) +1 = 2L+1. Se vogliamo dimostrare che le potenze di una base b hanno la stessa parità, non abbiamo che procedere ordinatamente. *Ad esempio, sia la base b un numero* ***dispari****. Il quadrato (prodotto di due numeri* ***dispari****) è un numero* ***dispari****, come abbiamo appena dimostrato. Il cubo sarà dato dal prodotto del quadrato, che è un numero* ***dispari*** *come dimostrato, per la base, che è* ***dispari*** *per ipotesi. Il risultato , prodotto di due numeri* ***dispari,*** *sarà ancora un bumero* ***dispari****. In questo modo si potrà procedere fino all'infinito.* Sostituendo nel ragionamento in corsivo la parola **dispari** con la parola **pari** si dimosterà che tutte le potenze di una base pari sono pari.

(**) La formula per il calcolo della ϕ di Euler di un qualsiasi numero (che ha sempre un'unica scomposizipne in fattori primi, cioè N = p1*p2*p3…) è come segue:

$\phi(N) = N (1-1/p1)(1-1/p2)(1- 1/p3 \ldots)$.

Per il numero 10, $\phi(10) = \phi(2*5) = 10 (1-1/2)(1-1/5) = 10 *(1/2)*4/5) = 40/10 = 4$.

(***) Questo può essere noto a chi fa il gioco di estrarre le radici quinte (esatte) di numeri fino a 99^5 (=9509900499). Ne ho scritto separatamente ieri in questo sito (https://dainoequinoziale.it/resources/scienze/matematica/radquadrate.pdf).