Il Teorema Cinese dei Resti

Luisella Caire, Umberto Cerruti
Politecnico e Università di Torino

12 Febbraio 2015

1 Perché cinese?

Il Teorema Cinese dei Resti (TCR) si occupa della soluzione di un sistema di congruenze lineari, o, equivalentemente, di trovare soluzioni intere per un insieme di equazioni di primo grado in due incognite del tipo $ax + by = c$, dove a, b, c, sono interi.

In Cina fin dal secondo secolo a.C. si studiavano i sistemi di congruenze, necessari per la determinazione dei calendari: una delle principali ragioni per studiare la matematica nell'antica Cina era proprio la determinazione del calendario.

La compilazione e la promulgazione del calendario era uno dei maggiori simboli dell'autorità imperiale. Il calendario di una dinastia doveva essere cambiato all'arrivo di una nuova dinastia (nel corso di 2000 anni furono cambiati più di 100 sistemi di calendari).

Nei palazzi imperiali allo scopo erano impiegati come ufficiali dell'impero molti scienziati: matematici, astronomi e astrologi.

I matematici erano incaricati di stabilire gli algoritmi per gli elaborati sistemi di calendari.

La gente comune aveva l'assoluta proibizione di costruire un sistema per definire il calendario e non poteva accedere alle conoscenze matematiche necessarie per studiare l'astronomia (e per i calendari). I dettagli tecnici sulla costruzione dei calendari dovevano essere mantenuti segreti.

Inoltre gli scienziati che stabilivano i calendari dovevano mantenere un alto grado di precisione, che era controllato a posteriori dalla coincidenza tra la posizione prevista per alcuni corpi celesti con quella che poi effettivamente avrebbero occupato nel corso degli anni successivi: succedeva sovente che alcuni calendari dovessero essere cambiati, ad esempio, perché non era stata predetta un eclisse solare.

I matematici impiegati come redattori di calendari in generale, non erano ricercatori matematici, ma si limitavano a elaborare i calcoli per i calendari. Lo scopo non era costruire modelli cosmici o geometrici dell'universo, né investigare sul moto dei corpi celesti, ma solo fornire metodi numerici per predire la posizione dei corpi celesti. Tranne pochi che lavoravano presso l'Osservatorio Imperiale, gli studiosi erano interessati alla matematica quasi solo per le sue applicazioni pratiche dell'astronomia ai calendari.

Il primo esempio di sistema di congruenze applicato ci è dato dal calendario del regno di *Jing Chu* (dinastia *Zhou*, 237 a.C.); gli astronomi definirono SHÀNGYUÁN (inizio degli anni) il punto di partenza del calendario: era il momento in cui coincidevano la mezzanotte di JIÀZI (il primo anno del ciclo di 60 anni), il solstizio d'inverno e la luna nuova.

Se il solstizio d'inverno di un certo anno cadeva r giorni dopo shàngyuán e s giorni dopo la luna nuova, allora quell'anno era N anni dopo shàngyuán ; di qui il problema di risolvere il sistema di congruenze

$$\begin{cases} aN \equiv r \bmod 60 \\ aN \equiv s \bmod b \end{cases}$$

dove a è il numero di giorni in un anno tropicale (per noi $a = 365$) e b il numero di giorni in un mese lunare (per noi $b = 28$).

Un problema aritmetico (ma anche pratico!) che comporta la soluzione di un sistema di congruenze si trova nel *Sūn Zi Suán Jīng* (Trattato di calcolo di *Sūn Zi* , III secolo d.C.), dove il problema 26 del terzo volume recita:

Vi sono certi oggetti il cui numero è ignoto;
se il numero è ripetutamente diviso per 3, il resto è 2;
se diviso per 5, il resto è 3 ;
se diviso per 7, il resto è 2.
Qual è questo numero?

Una versione aneddotica del problema è nota come *L'imperatore conta segretamente i suoi soldati*: se li conta a gruppi di 3, ne restano fuori 2; se li conta a 5 a 5, ne rimangono 3; se li raduna a gruppi di 7, ne avanzano 2 fuori dal gruppo.

La formulazione matematica del problema può essere così espressa: cercare un numero x tale che

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases}$$

Sūn Zi risolse il problema, trovando

$$x = 140 + 63 + 30 = 233 \equiv 23 \pmod{105}$$

Per spiegare l' algoritmo che produce gli addendi della sua soluzione egli scrisse:

si cerchi prima G_1 per cui

$$G_1 \equiv 0\,(\mathrm{mod}5), \quad G_1 \equiv 0\,(\mathrm{mod}7), \quad G_1 \equiv 1\,(\mathrm{mod}3)\ ;$$

si prenda $G_1 = 70$.
Si cerchi ora G_2 tale che

$$G_2 \equiv 0\,(\mathrm{mod}3), \quad G_2 \equiv 0\,(\mathrm{mod}7), \quad G_2 \equiv 1\,(\mathrm{mod}5)\ ;$$

si prenda $G_2 = 21$.
Si cerchi infine G_3 per cui

$$G_3 \equiv 0\,(\mathrm{mod}3), \quad G_3 \equiv 0\,(\mathrm{mod}5), \quad G_3 \equiv 1\,(\mathrm{mod}7)\ ;$$

si prenda $G_3 = 15$.

Ora, per risolvere il presente problema, si cerchino

$$G_1' \equiv 0\,(\mathrm{mod}5), \quad G_1' \equiv 0\,(\mathrm{mod}7), \quad G_1' \equiv 2\,(\mathrm{mod}3);$$

si prenda $G_1' = 70 \times 2 = 140$

$$G_2' \equiv 0\,(\mathrm{mod}3), \quad G - 2' \equiv 0\,(\mathrm{mod}7), \quad G_2' \equiv 3\,(\mathrm{mod}5)$$

si prenda $G_2' = 21 \times 3 = 63$.

$$G_3' \equiv 0\,(\mathrm{mod}3), \quad G_3' \equiv 0\,(\mathrm{mod}5), \quad G_3' \equiv 2\,(\mathrm{mod}7)$$

si prenda $G_3' = 15 \times 2 = 30$.

Allora il valore cercato è

$$x = G_1' + G_2' + G_3'\,(\mathrm{mod}\ 105)$$

L'esempio di Sūn Zi è un caso numerico speciale, che può essere generalizzato così : determinare un numero x tale che

$$x \equiv a_i\ (\mathrm{mod}\, m_i)\,(i = 1, 2, \ldots, n)$$

dove

$$MCD(m_i, m_j) = 1, \quad 1 \leq i < j \leq n$$

Siano

$$G_i \equiv 0\,(\mathrm{mod}\ m_j), \quad \text{per ogni } i \neq j, \quad \text{e} \quad G_i \equiv 1\,(\mathrm{mod}\ m_i)$$

allora, posto

$$M = \prod m_i, \quad M_i = \frac{M}{m_i}$$

si ha

$$x = \sum G_i' = \sum G_i a_i\,(\mathrm{mod}\ M)$$

In termini moderni, la soluzione è data da

$$x = \sum_{i=1}^{n} a_i F_i M_i$$

in cui F_i è l' inverso modulare di $M_i\,(\mathrm{mod}\ m_i)$, cioè $G_i = M_i F_i = 1\,(\mathrm{mod}\ m_i)$.

Questo è il Teorema di Sūn Zi o **Teorema Cinese dei Resti**.

Il teorema ha preso questo nome, non solo perché formulato da Sūn Zi e risolto dagli antichi matematici Cinesi (era forse noto anche ai Greci ancor prima che ai Cinesi), ma anche come riconoscimento ai Cinesi per i loro contributi alla teoria dei numeri.

Sūn Zi diede per primo la risposta a questo problema, trovando l'algoritmo sopra esposto, ma senza spiegare la regola generale, né dimostrare perché funzionava.

Il primo che sviluppò la teoria nel caso generale fu *Qín Jiŭsháo* nel 1247, nel suo libro SHÙSHŪ JIŬZHĀNG (SSJZ) (Trattato matematico in 9 capitoli). Qín Jiŭsháo sviluppò la teoria generale per risolvere i sistemi di congruenze lineari

$$x \equiv a_i \,(\mathrm{mod}\, m_i)$$

e chiamò la sua tecnica DÀ YĂN QIÚ YĪSHÙ (tecnica della grande estensione per la ricerca dell'unità), o anche semplicemente DÀ YĂ*n* SHÙ.

Ricordiamola:

1. Ridurre i moduli m_i (detti DÌ NG) a prodotti o potenze di primi, a meno che non siano già essi stessi primi (come nell'esempio di Sūn Zi) o potenze di primi. I moduli relativamente primi sono detti DÌ NG SHÙ.

2. Trovare il minimo comune multiplo m dei moduli, detto YĂN (sviluppo). Nel suo esempio $m = 3 \times 5 \times 7 = 105$.

3. Dividere lo yăn m per tutti i dì ng shù. I risultati sono detti YĂN SHÙ : nell'esempio sono 35, 21 e 15 rispettivamente.

4. Sottrarre dagli yăn shù i corrispondenti dì ng shù quante volte possibile. I resti s_i sono detti QÍSHU (numeri del destino: il perché si vedrà in seguito).
   Nell'esempio $35 - 3 \times 11 = 2 = s_1$, $21 - 5 \times 4 = s_2$, $15 - 7 \times 2 = 1 = s_3$

5. Calcolare i CHÉNGLÙ (termini rivelatori) b_i in modo tale che $s_i \times b_i = 1 \,(\mathrm{mod}\ m_i)$
   Nell'esempio $2b_1 \equiv 1 \,(\mathrm{mod}\ 3)$, da cui $b_1 = 2$, $b_2 \times 1 \equiv 1 \,(\mathrm{mod}\ 5)$, da cui $b_2 = 1$ e $b_3 \times 1 \equiv 1 \,(\mathrm{mod}\ 7)$, per cui $b_3 = 1$.

6. Moltiplicare i chénglù con i corrispondenti yăn shù. Questi sono detti YÒNG SHÙ (numeri utili). Nell'esempio: $2 \times 35 = 70$, $1 \times 21 = 21$ and $1 \times 15 = 15$.

7. Moltiplicare gli yòng shù con i qì shù. Nell'esempio $70 \times 2 = 140$, $21 \times 3 = 63$ e $15 \times 2 = 30$.

8. Sommando insieme i prodotti, si otterrà lo ZŎNG SHÙ (numero totale, somma) dunque $140 + 63 + 30 = 233$.

9. Sottraendo da questa somma lo yăn m quante volte possibile si avrà infine la soluzione, $x = 233 - 105 - 105 = 23$.

Qín Jiŭsháo ci indica numerose applicazioni del dà yăn nel campo dei problemi amministrativi. Ma l'interesse per i sistemi di congruenze è legato anche all'arte degli oroscopi, importantissima per i cinesi: nel libro YÌ JĪNG (o I CHING, Libro dei mutamenti), viene richiesto di dividere un numero di bastoncini (meno uno) in due gruppi, che simboleggiano lo *Yīn* e lo *Yáng*, i due elementi duali per l'armonia dell'universo.

La versione più popolare degli oroscopi, per cui serve risolvere un sistema di congruenze, può essere di questo tipo: ogni mattina il signor Wáng si reca dal suo indovino personale per farsi fare l'oroscopo della giornata.

L'indovino ha in mano un mazzo di bastoncini, e trarrà da questi indicazioni per il suo cliente:

- sull'andamento degli affari nella giornata, raccogliendo i bastoncini a 3 a 3 e contando il resto (0=pessima giornata, 1= mediocri affari, 2= ottima giornata);
- sullo stato di salute del signor Wáng; raccoglie i bastoncini a 5 a 5 e conta i resti: 0=pessima salute, 1=cattiva salute, 2=mediocre, 3=buona, 4=in gran forma);
- sul numero dei nemici che dovrà affrontare (raccoglie i bastoncini a 7 a 7, il resto rappresenta il numero di persone ostili da affrontare).

Chiaramente un indovino che vuole propiziarsi il cliente farà in modo che il numero di bastoncini dia i resti a lui più favorevoli: il miglior risultato lo avrà se il numero N dei bastoncini sarà congruo a $2 \pmod 3$, congruo a $4 \pmod 5$, e se sarà multiplo di 7. Dovrà dunque risolvere il sistema di congruenze

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 4 \bmod 5 \\ x \equiv 0 \bmod 7 \end{cases}$$

Lo studio delle congruenze lineari fu molto sviluppato anche in India; la leggenda narra che *Āryabhata* (476-550 d.C.) pose il problema di determinare un intero N che diviso per a lascia resto r, mentre diviso per b, dà come resto s; cioè cercava le soluzioni del sistema di congruenze

$$\begin{cases} x \equiv r \bmod a \\ x \equiv s \bmod b \end{cases}$$

ovvero cercava N tale che

$$\begin{cases} N = ax + r \\ N = by + s \end{cases}$$

e quindi doveva risolvere l'equazione diofantea $by - ax = c$, dove $c = r - s$.

Āryabhata scoprì una regola per trovare la soluzione, che egli indicò in due oscure strofe del suo *Āryabhaṭīya*.

Anche *Brāhmagupta* (598-670 d. C.) studiò intensivamente le congruenze e intitolò KUTTAKA uno dei capitoli del *Siddhānta* (628 d.C.): Kuttaka significa polverizzatore, in riferimento al processo di divisioni iterate adottato per trovare le soluzioni delle congruenze, che trova spezzando via via i numeri: si tratta dell'algoritmo euclideo del Massimo Comun Divisore Esteso che spiegheremo nel prossimo paragrafo.

Brāhmagupta, come i cinesi, non era interessato soltanto agli aspetti teorici delle congruenze, ma ne aveva bisogno per risolvere calcoli astronomici; ad esempio, utilizzando i

sistemi di congruenze studiò il numero di giorni che occorrono ai corpi celesti per completare un'intera rivoluzione intorno ad altri corpi fissi.

2 L'algoritmo di Euclide e l'identità di Bezout

Dati due interi positivi $a, b \in \mathbb{N}$, consideriamo l'equazione diofantea (detta identità di Bezout)

$$ax + by = m \tag{1}$$

La (1) ha soluzione $x, y \in \mathbb{Z}$ se e solo se $d|m$, dove d è il massimo comun divisore (a, b) di a e b.

Se la coppia (x, y) è una soluzione, anche la coppia $(x + bk, y - ak)$ è una soluzione, per qualsiasi $k \in \mathbb{Z}$.

Pertanto la (1) possiede 0 oppure infinite soluzioni.

La $ax + by = d$, dove $d = (a, b)$, si può risolvere con l'algoritmo di Euclide esteso.

Cominciamo con l'algoritmo di Euclide.

Sappiamo che non esistono algoritmi veloci per fattorizzare un numero. Non sappiamo pertanto trovare i divisori di un intero grande. L'algoritmo di Euclide svolge un compito apparente impossibile. Dati due interi a, b, determina il più grande dei loro divisori comuni, senza conoscere né i divisori di a, né quelli di b. Non è incredibile?

L'algoritmo di Euclide si basa, a sua volta, sull'algoritmo della divisione.

Dati due interi $a, b \in \mathbb{Z}$, con $b \neq 0$, esistono, e sono *unici*, due interi $q \in \mathbb{Z}$ e $r \in \mathbb{N}$, tali che valgano le due seguenti condizioni:

1. $0 \leq r < |b|$
2. $a = qb + r$

L'intero r viene detto resto della divisione (mentre, come sappiamo, q è il quoziente).

Quello che ci interessa del resto è il fatto che, se r non è nullo, allora r è un intero positivo strettamente inferiore a b.

Supponiamo $a > b > 0$.

Il motore dell'algoritmo di Euclide è la seguente constatazione

$$(a, b) = (b, r) \tag{2}$$

dove r è il resto della divisione di a per b.

Il calcolo del massimo comun divisore tra a e b equivale pertanto al calcolo del massimo comun divisore tra b e r, dove

$$b < a \quad r < b$$

Si passa quindi da una coppia di interi ad un'altra coppia i cui elementi sono entrambi strettamente minori dei precedenti.

Poiché i numeri non sono mai negativi, il procedimento di sostituzione termina in un numero finito di passi.

Precisamente, posti $r_0 = a$ e $r_1 = b$, si effettua una catena di divisioni dove i q_i sono i quozienti e gli r_i sono i resti.

$r_0 = q_0 r_1 + r_2$
$r_1 = q_1 r_2 + r_3$
$\cdots$
$r_k = q_k r_{k+1} + r_{k+2}$
$\cdots$
$r_{n-1} = q_{n-1} r_n + 0$

Si ottiene così, dalla (2),che

$$(a, b) = (b, r_2) = (r_2, r_3) = \cdots = (r_k, r_{k+1}) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n$$

Pertanto il massimo comun divisore tra a e b è l'ultimo resto non nullo r_n.

Poiché $q_k \geq 1$ ha sempre

$$r_k \geq r_{k+1} + r_{k+2}$$

e poiché $r_{k+2} < r_{k+1}$

$$r_k > 2r_{k+2}$$

ovvero

$$r_{k+2} < \frac{r_k}{2}$$

e quindi, nel peggiore dei casi, il resto si dimezza ogni due passi!

L'algoritmo di Euclide è veloce! Termina in un numero di passi che è al massimo $[\log_2(n)] + 1$.

Un piccolo esempio, con $a = 63$ e $b = 29$.

$63 = 2 \times 29 + 5$
$29 = 5 \times 5 + 4$
$5 = 1 \times 4 + 1$
$4 = 4 \times 1 + 0$

Questo prova che $(63, 29) = 1$.

Naturalmente questo si vedeva senza bisogno di algoritmi particolari.

Cosideriamo ora $a = 1171781605876266$ e $b = 292587159746095$. Calcolando il logaritmo in base 2 di b troviamo $48,05\ldots$. Sappiamo allora che in al più 49 passi l'algoritmo di Euclide termina e ci dà (a, b).

Però quello è il caso peggiore. Eseguendo l'algoritmo di Euclide, in questo caso, arriviamo alla fine in 12 passi. La successione dei resti è

1171781605876266, 292587159746095, 1432966891886, 261913801351, 123397885131, 15118031089, 2453636419, 396212575, 76360969, 14407730,4322319, 1440773, 0

Pertanto $(a, b) = 1440773$.

L'algoritmo *esteso* di Euclide, restituisce non soltanto $d = (a, b)$, ma anche x, y tali che

$$xa + yb = d$$

L'idea è quella di partire con le identità banali

$$1 \times a + 0 \times b = a$$

$$0 \times a + 1 \times b = b$$

e di portarle avanti, parallelamente alla applicazione dell'algoritmo di Euclide, mantenendo ad ogni passo u

$$h \times a + k \times b = r_u$$

dove $r_0 = a$, $r_1 = b$, e l'ultimo r_u non nullo è proprio d.

Eseguiamo i passaggi nel caso $a = 63$, $b = 29$.

All'inizio abbiamo

$$r_0 : \qquad 1 \times 63 + 0 \times 29 = 63$$

$$r_1 : \qquad 0 \times 63 + 1 \times 29 = 29$$

Dividiamo 63 per 29 e otteniamo $5 = 63 - 2 \times 29$.

Calcoliamo $r_0 - 2 \times r_1$ e otteniamo

$$r_2 : \qquad 1 \times 63 - 2 \times 29 = 5$$

Dividiamo 29 per 5 e otteniamo $4 = 29 - 5 \times 5$.

Calcoliamo $r_1 - 5 \times r_2$ e otteniamo

$$r_3 : \qquad -5 \times 63 + 11 \times 29 = 4$$

Infine $r_4 = r_2 - r_3$.

Il tutto si può mettere sotto forma di tabella, composta dalle righe $R_0, \cdots R_4$

R_0	63	1	0
R_1	29	0	1
R_2	5	1	-2
R_3	4	-5	11
R_4	1	6	-13

L'algoritmo per il calcolo del massimo comun divisore esteso di a e b è un algoritmo ricorsivo. La riga k-esima viene calcolata utilizzando le righe $k-1$ e $k-2$.

La inizializzazione consiste nelle due righe

R_0	$r_0 = a$	1	0
R_1	$r_1 = b$	0	1

Supponiamo di avere calcolato tutte le righe fino alla riga $k-1$. Cosideriamo le righe R_{k-2} e R_{k-1}.

R_{k-2}	r_{k-2}	u_{k-2}	v_{k-2}
R_{k-1}	r_{k-1}	u_{k-1}	v_{k-1}

Questo significa che

$$r_{k-2} = u_{k-2}a + v_{k-2}b$$

e

$$r_{k-1} = u_{k-1}a + v_{k-1}b$$

Eseguendo l'algoritmo di Euclide avremo ottenuto nel frattempo

$$r_{k-2} = q_{k-2}r_{k-1} + r_k$$

e quindi

$$r_k = r_{k-2} - q_{k-2}r_{k-1}$$

Consegue che $R_k = R_{k-2} - q_{k-2}R_{k-1}$, e si ottiene la riga R_k

R_k	r_k	$u_{k-2} - q_{k-2}u_{k-1}$	$v_{k-2} - q_{k-2}v_{k-1}$

Ovvero, $u_k = u_{k-2} - q_{k-2}u_{k-1}$ e $v_k = v_{k-2} - q_{k-2}v_{k-1}$ e

$$r_k = u_k a + v_k b$$

Infine giunti all'ultima riga R_n, avremo $r_n = (a, b)$ e

$$(a, b) = u_n a + v_n b$$

Torniamo allora alla equazione diofantea (1).

Poniamo $d = (a, b)$. Se d non divide m non ci sono soluzioni. Se invece $m = kd$, con il metodo visto si trovano u, v tali che

$$d = ua + vb$$

e pertanto

$$m = xa + yb$$

dove $x = ku$ e $y = kv$.

Esempio 1.
Risolvere l'equazione diofantina

$$63x + 29y = 2014$$

Soluzione

Utilizziamo l'algoritmo esteso di Euclide.
Troviamo

$$6 \times 63 - 13 \times 29 = 1$$

Dunque

$$(6 \times 2014) \times 63 - (13 \times 2014) \times 29 = 2014$$

Segue che una soluzione è

$$x = 12084,\ y = -26182$$

In particolare abbiamo dimostato che se $(a, b) = 1$, allora esistono due interi h, k tali che la identità di Bezout

$$ha + kb = 1 \tag{3}$$

è soddisfatta.

Inoltre siamo in grado di calcolare h, k con l'algoritmo di Euclide esteso.

3 La funzione di Eulero e l'inversione modulare

Ricordiamo che la funzione di Eulero $\varphi(n)$ conta il numero degli interi che precedono n e sono coprimi con n.

$$\varphi(n) = |\{a \leq n : (a, n) = 1\}|$$

Poniamo

$$\mathbb{Z}_n = \{0, 1, \cdots n-1\}$$

In $\mathbb{Z}_n$ sono definite in modo naturale le operazioni di somma e prodotto modulo n.

Infatti $\mathbb{Z}_n$ è l'insieme di tutti i possibili resti di una divisione per n. Dati a, b in $\mathbb{Z}_n$, la somma e il prodotto modulo n sono dati dai resti delle divisioni di $a + b$ o di ab per n.

In $\mathbb{Z}_n$ alcuni elementi sono invertibili e altri no. Per esempio in $\mathbb{Z}_{30}$ 9 non è invertibile, mentre 7 ha inverso 13.

Infatti

$$7 \times 13 = 91 = 1 \bmod 30$$

Gli elementi invertibili si possono facilmente caratterizzare.

Utilizzeremo un teorema (di Eulero) estremamente utile

Teorema 2.

$$(a, n) = 1 \Rightarrow a^{\varphi(n)} = 1 \, mod \, n$$

Teorema 3.

Dato $a \in \mathbb{Z}_n$, a è invertibile se e solo se

$$(a, n) = 1$$

Dimostrazione. Supponiamo a invertibile. Allora esiste un b tale che

$$ab \equiv 1 \bmod n$$

ovvero

$$ab = 1 + kn$$

Da questa si deduce che se d divide sia a che n allora d divide 1. Pertanto a, n sono coprimi.

Supponiamo ora

$$(a, b) = 1$$

.

Per il Teorema di Eulero (2)

$$a^{\varphi(n)} = 1 \bmod n$$

Segue che $a^{\varphi(n)-1}$ è l'inverso di a modulo n in quanto

$$a^{\varphi(n)-1}a = a^{\varphi(n)} = 1 \bmod n$$

□

La dimostrazione del teorema (3) è costruttiva, nel senso che l'inverso di a viene determinato esplicitamente, non ci si lmita a provarne la esistenza.

Per trovare l'inverso di a è sufficiente calcolare $\varphi(n)$. Se la decomposizione di n in fattori primi è

$$n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} \tag{4}$$

allora si prova che

$$\varphi(n) = \prod_{k=1}^{t} \varphi(p_k^{e_k})$$

Inoltre si ha che, se p è primo

$$\varphi(p^e) = p^{e-1}(p-1)$$

Il metodo però non è efficace, perché per calcolare $\varphi(n)$ occorre conoscere i fattori di n, e non siamo a tutt'oggi in grado di fattorizzare interi grandi.

Esiste un metodo assai veloce, basato sull'algoritmo di Euclide.

Per la identità di Bezout (3) esistono h, k interi tali che

$$ha + kn = 1$$

Leggiamo questa uguaglianza modulo n. Poiché

$$n = 0 \bmod n$$

essa diventa

$$ha = 1 \bmod n$$

Pertanto h è l'inverso di a modulo n.

$$h = a^{-1} \bmod n$$

Con il metodo visto nel paragrafo 2, h si calcola facilmente anche per interi molto grandi.

Siamo ora in grado di fabbricare un algoritmo che fornisce le soluzioni del sistema di congruenze lineari che appare nel Teorema Cinese dei Resti.

Teorema 4. *Siano date k conguenze lineari*

$$x \equiv a_i \, mod \, n_i \quad 1 \leq i \leq k \tag{5}$$

dove gli n_i sono a due a due coprimi.
Sia

$$n = \prod_{i=1}^{k} n_i$$

Si ponga

$$M_i = \frac{n}{n_i}$$

$$T_i = M_i^{-1} \, mod \, n_i$$

Allora

$$x = \sum_{i=1}^{k} M_i T_i a_i$$

è soluzione del sistema.
Inoltre x è la sola soluzione modulo n

Dimostrazione. Osserviamo che

$$\forall \, i \quad (M_i, n_i) = 1$$

Per questo motivo esiste sempre T_i, l'inverso di M_i modulo n_i.

Inoltre

$$i \neq j \; \Rightarrow \; n_j | M_i$$

Pertanto se fissiamo un j e vediamo x modulo n_j, tutti gli $M_i T_i$ con $i \neq j$ si annullano e rimane

$$x = M_j T_j a_j = M_j M_j^{-1} a_j = a_j \bmod n_j$$

Quindi x è soluzione del sistema (5).

Supponiamo che anche y sia una soluzione.

Allora

$$\forall j \quad x \equiv y \bmod n_j$$

Segue che, per ogni j, n_j divide la differenza $x - y$. Poiché gli n_j sono coprimi, il loro prodotto n divide $x - y$ e si ha

$$x \equiv y \bmod n$$

che prova la unicità della soluzione modulo n.

□

Il sistema (5) ha soluzione anche quando i moduli n_i non sono coprimi, posto che valga una certa condizione.

Precisamente si ha ([6])

Teorema 5. *Il sistema (5) ha soluzione se e solo se*

$$\forall \, i, j \quad a_i \equiv a_j \, mod \, (n_i, n_j) \tag{6}$$

Quando la soluzione esiste, essa è unica modulo il minimo comune multiplo dei moduli.

Il TCR è uno strumento fondamentale e ha innumerevoli applicazioni.

Tra l'altro il TCR permette il calcolo parallelo, spezzando un problema in un numero finito di problemi indipendenti, che possono essere risolti singolarmente.

Un esempio classico è il problema di trovare le soluzioni di

$$f(x) \equiv 0 \bmod n \quad (*)$$

dove $f(x) \in \mathbb{Z}$ è un polinomio con i coefficienti interi.

Se la fattorizzazione di n (4) è nota, allora si risolvono separatamente le t equazioni

$$f(x) \equiv 0 \bmod p_i^{e_i}$$

determinando, per ognuna di esse, v_i soluzioni

$$w_{i,1}, w_{i,2}, \cdots, w_{i,v_i}$$

Se uno dei v_i è 0 la $(*)$ non ha soluzioni.

Altrimenti possiede $v = \prod_{i=1}^{t} v_i$ soluzioni $z_{j_1,j_2,\ldots,j_t}$, dove

$$1 \leq j_k \leq v_k \quad 1 \leq k \leq t$$

Per trovare $z_{j_1,j_2,\ldots,j_t}$ si utilizza il TCR risolvendo il sistema

$$z \equiv w_{i,j_i} \bmod p_i^{e_i} \quad 1 \leq i \leq t$$

Facciamo un esempio.

Esempio 6.

Cosideriamo $f(x) = x^2 - a$ e $n = pq$, con p, q primi.

Supponiamo che la

$$f(x) \equiv a (\bmod\ n)$$

abbia soluzioni.

Questo equivale a dire che possiede soluzioni sia modulo p che modulo q.

Siano $\pm w$ le due soluzioni modulo p e $\pm z$ quelle modulo q.

Quindi, per quanto detto sopra, la equazione

$$x^2 \equiv a \bmod n$$

ha 4 soluzioni.

Esse si ottengono con il TCR risolvendo 4 sitemi lineari.

In realtà è sufficiente risolverne 2

$$\begin{cases} u \equiv w \bmod p \\ u \equiv z \bmod q \end{cases}$$

e

$$\begin{cases} v \equiv w \bmod p \\ v \equiv -z \bmod q \end{cases}$$

Le soluzioni modulo n saranno pertanto $\pm u$, $\pm v$.

Si noti che le 4 soluzioni vengono a coppie.
Diciamo che due soluzioni s, t sono *essenzialmente diverse* se

$$s \not\equiv \pm t \bmod n$$

Nell'esempio appena fatto u, v sono una coppia di soluzioni essenzialmente diverse.

Vediamo una applicazione ad un interessante protocollo crittografico, dovuto a Manuel Blum ([2]).
Il protocollo utilizza due fatti.
Primo:

Teorema 7.
Sia p un numero primo congruo a 3 modulo 4.
Supponiamo che l'equazione

$$x^2 \equiv a \, mod \, p \quad (\iota)$$

possieda soluzioni.
Allora le soluzioni sono

$$\pm a^{\frac{p+1}{4}}$$

Osservazione 8. *Esiste un algoritmo efficiente, ma più complicato, per risolvere l'equazione (ι) anche quando p è congruo a 1 modulo 4.*

Secondo:

Teorema 9.
Supponiamo $n = pq$.
Sono equivalenti:

1. *Conoscere due soluzioni essenzialmente diverse della equazione*

$$x^2 \equiv a \, mod \, n$$

2. *Conscere i fattori p e q di n.*

Dimostrazione. Supponiamo verificata la 1.
Conosco allora due soluzioni u, v essenzialmente diverse. Quindi

$$u^2 \equiv a \bmod n$$

$$v^2 \equiv a \bmod n$$

pertanto

$$u^2 \equiv v^2 \bmod n$$

Questo significa che n divide $u^2 - v^2$, e, consegentemente,
$n \mid (u - v)(u + v)$
Sia $d = (n, u - v)$.

Se fosse $d = 1$, n sarebbe coprimo con $u - v$, e quindi n dovrebbe dividere $u + v$. Si avrebbe allora

$$u \equiv -v \bmod n$$

che non può essere.

Se poi si avesse $d = n$, allora n dividerebbe $u - v$ e quindi

$$u \equiv v \bmod n$$

che è del pari impossibile.

Dunque d è un fattore proprio di n. Avremo pertanto $d = p$, oppure $d = q$. L'altro fattore si trova dividendo.

Supponiamo verificata la 2.

Conosco p, q e posso allora (vedi il Teorema 7 e la Osservazione (8)) trovare le soluzioni della equazione modulo p e modulo q. Da queste, come sappiamo, si risale alle soluzioni modulo n. □

4 Lancio di una moneta al telefono

Alice e Bob sono innamorati ma lontani, Alice vive a Roma e Bob a Sidney. Parlano su Skype.

Bob: Vieni a trovarmi nelle vacanze
Alice: Preferirei che venissi tu qui, è più bello ...
Bob: Lo sai che non mi piace viaggiare! Facciamo così. Lancio una moneta.
Se viene testa sabato parto. Altrimenti tocca a te. Fatto! E' venuta croce.
Alice: Mmmm, non mi convince.
Bob: Lo sai che non ti mentirei mai.
Alice: Sì certo. Però, per essere proprio sicura facciamo così ...

Io calcolo due primi grandi p, q congrui a 3 modulo 4.
Bob: Quanto grandi?
Alice: Grandi abbastanza che tu non sia in grado di fattorizzare il loro prodotto n, se non teli dico. Diciamo un centinaio di cifre decimali ciscuno.
Bob: Accidenti!
Alice: Poi faccio il prodotto $n = pq$ e te lo mando.
Bob: E io che me ne faccio?
Alice: Tu calcoli un b casuale tale che $b^2 > n$, lo conservi, e mi spedisci

$$a = b^2 \bmod n$$

Bob: Cioè ti mando il resto della divisione di b^2 per n.

Alice: Esatto. Questo a che mi hai inviato, per costruzione è un quadrato, sia modulo p che modulo q.

Io conosco i due primi, e quindi posso trovare le soluzioni

$$w = a^{\frac{p+1}{4}} \bmod p$$
$$z = a^{\frac{q+1}{4}} \bmod q$$

Da queste risalgo alle due coppie di soluzioni modulo n, essenzialmente diverse.

Bob: E come fai?

Alice: Uso il Teorema Cinese dei Resti, è chiaro.

Bob: Beata te.

Alice: Comunque ho queste due coppie $\pm u$, $\pm v$.

Poiché il b che avevi calcolato soddisfa la

$$b^2 \equiv a \bmod n$$

e ci sono soltanto 4 soluzioni, che si presentano a coppie, una tra le coppie $\pm u$ e $\pm v$ sarà la coppia $\pm b$.

Ma io non posso sapere qual è, tra le due.

Bob: Vedi, anche tu non sai tutto...

Alice: Purtroppo. Non potrò sapere la coppia giusta da inviarti.

Bob: Giusta per far cosa?

Alice: Per farti perdere.

Bob: Grazie, come sei cara...

Alice: A testa o croce uno deve pur predere.

Bob: Sì, ma io come vinco?

Alice: Aspetta. Tu per vincere devi fattorizzare n, il numero che ti ho mandato all'inizio.

Bob: Bene, benissimo! Forse con una rete di computer e qualche anno a disposizione e apposito software...

Alice: Non ce la faresti nemmeno così.

Bob: Allora dimmi che devo venire per forza, e la facciamo finita con questa farsa.

Basta!

Alice: Non ti arrabbiare. Tu puoi farcela.

Puoi farcela se io ti mando la coppia sbagliata, sbagliata per me capisci?

Bob: No.

Alice: Supponiamo che la coppia $\pm u$ sia la $\pm b$. E che io, disgraziatamente, decida di spedirti l'altra, la $\pm v$.

Bob: Non so che farmene.

Alice: Tu, utilizzando la coppia $\pm v$ fattorizzi n, e vinci!

Vinci se e solo se fattorizzi n.

Lo puoi fare se e solo se io ti mando la coppia $\pm v$.

Per me sono solo dei numeri grandi, non ho nessuna possibilità di riconoscere $\pm b$. In effetti farò così per scegliere. Lancerò una moneta vera, e deciderò in conseguenza.

Bob: Te lo ripeto, anche se tu mi mandi $\pm v$, io non so come fattorizzare quel benedetto numero.

Alice: Sei in grado di calcolare il massimo comun divisore di due interi grandi?

Bob: Certo. Ho Pari/Gp sul computer. Posso usare la funzione *gcd*, è velocissima, anche con numeri di migliaia di cifre.

Alice: Benissimo. Riassumendo:

Io estraggo una delle due coppie a caso e te la mando.

Se tu vedi che è quella che già conosci, $\pm b$ hai perso. Non puoi fingere

Bob: Non fingerei mai!

Alice: di avere vinto. La prova della vittoria sono i fattori p e q.

Se invece ricevi l'altra coppia $\pm v$ calcoli

$$gcd(n, b - v)$$

e fattorizzi n.

Bob: Ora ho capito! Fantastico! Facciamolo subito, ho qui il computer.

(eseguono il protocollo)

Bob: Ho vinto! Ecco i fattori!

Alice: Si vede che era destino. Comunque è stato divertente.

Sabato parto e domenica sono da te! Ciao amore!

Bob: Che bello! Ti preparo un bel pranzetto. Ciao gioia!

Il lancio della moneta al telefono è un protocollo crittografico molto importante.

Vediamo ora tre applicazioni, non usuali, del TCR alla teoria dei numeri.

5 TCR e Teorema di Wilson

Nella teoria dei numeri è noto, tra gli altri, un particolare quoziente, detto *quoziente di Wilson*.

Ricordiamo il Teorema di Wilson

Teorema 10. *L'intero n è primo se e solo se*

$$(n-1)! \equiv -1 \, mod \, n$$

Da questo si ottiene immediatamente

Corollario 11. *L'intero n è primo se e solo se*

$$n \mid (n-1)! + 1$$

Dato un primo p è dunque definito il quoziente

$$W(p) = \frac{(p-1)! + 1}{p} \tag{7}$$

Se calcoliamo $W(p)$ con p primo, $p = 2, 3, 5, \ldots$, otteniamo

$$1, 1, 5, 103, 329891, 36846277, 1230752346353, 336967037143579, \cdots \tag{8}$$

E' la sequenza A007619.
Se $W(p)/p$ è intero, allora p si dice *primo di Wilson*.
Si pensa che ci siano infiniti primi di Wilson, ma soltanto tre sono noti

$$5, 13, 563$$

e non ce ne sono altri fino a $2\,10^{13}$.

Vediamo come si connette tutto questo con il TCR.
L'intero $z = (p-1)! + 1$ soddisfa le congruenze

$$\begin{cases} z \equiv 0 \bmod p \\ z \equiv 1 \bmod p - 1 \\ z \equiv 1 \bmod p - 2 \\ \cdots \\ z \equiv 1 \bmod 2 \end{cases} \tag{9}$$

Per il Teorema (5) il sistema (9) ha soluzioni, e queste, ovviamente, sono le stesse del sistema

$$\begin{cases} z \equiv 0 \bmod p \\ z \equiv 1 \bmod \nu(p-1) \end{cases} \tag{10}$$

dove si è posto (mcm è il minimo comune multiplo)

$$\nu(m) = mcm(1, 2, 3, \ldots, m)$$

Questo è l'inizio della sequenza $\nu(n)$

$$1, 2, 6, 12, 60, 60, 420, 840, 2520, 2520, 27720, 27720, \cdots$$

E' la sequenza A003418.

Al variare di p nell'insieme dei primi, le soluzioni non negative minime $z = \theta(p)$ di (10) sono

$$0, 3, 25, 301, 25201, 83161, 7207201, 49008961, 698377681, 2248776129601, \cdots$$

A parte il termine iniziale è la A094998.

Un analogo del quoziente di Wilson è pertanto la successione

$$W_1(p) = \frac{\theta(p)}{p}$$

I termini iniziali di $W_1(p)$ sono

$$0, 1, 5, 43, 2291, 6397, 423953, 2579419, 30364247, 77544004469, \cdots$$

A parte il termine iniziale è la A099794.

Tra i primi 1000 primi gli unici p tali che $W_1(p)/p$ sia intero sono 2, 5 e 31. Infatti si ha

$$W_1(2) = 0$$

$$W_1(5) = 5$$

$$W_1(31) = 31 \times 839 \times 49107719$$

Se studiamo bene il metodo di soluzione del TCR visto in (4) scopriamo che la soluzione $\theta(p)$ è

$$\theta(p) = (p^{-1} \bmod \nu(p-1))p$$

Pertanto si ha

$$W_1(p) = p^{-1} \bmod \nu(p-1)$$

La successione dei quozienti $W_1(p)$ è semplicemente la sequenza il cui n-esimo elemento è l'inverso dell'n-esimo primo modulo il minimo comune multiplo degli interi che lo precedono!

Ricordiamo che la soluzione di (10) è unica modulo il minimo comune multiplo dei moduli p e $\nu(p-1)$. Dunque è unica modulo $\nu(p)$.

Ne consegue che, poiché gli interi $(p-1)! + 1$ e $\theta(p)$ sono entrambi soluzioni, la loro differenza deve essere divisibile per $\nu(p)$.

Poniamo

$$W_2(p) = \frac{(p-1)! + 1 - \theta(p)}{\nu(p)}$$

La sequenza $W_2(p)$ è

$$1, 0, 0, 1, 130, 1329, 1707670, 27502484, 209927657739, 130904517147542068, \cdots$$

Questa sequenza non è in $OEIS$.

Se ritorniamo al sistema (10), vediamo che la soluzione $\theta(p)$ è il più piccolo intero naturale divisibile per p che dà sempre resto 1 quando lo si divida per $2, 3, \ldots, p-1$.

Consideriamo il problema duale. Prendiamolo come un gioco, un puzzle.

Sia p un numero primo. Cerchiamo un numero di palline n tale che raggruppando le palline a 2 a 2, a 3 a 3, $\cdots$ a $p-1$ a $p-1$ non avanzi nulla, mentre ragguppandole a p a p ne avanzi esattamente una.

Vogliamo dunque risolvere il sistema

$$\begin{cases} z \equiv 1 \bmod p \\ z \equiv 0 \bmod \nu(p-1) \end{cases} \tag{11}$$

Si vede subito che ora la soluzione è

$$\eta(p) = (\nu(p-1)^{-1} \bmod p)\nu(p-1)$$

La successione $\eta(p)$, con p primo, inizia con

$$1, 4, 36, 120, 2520, 277200, 5045040, 183783600, 4655851200, 80313433200, 32607253879200, \cdots$$

Sappiamo che $\eta(p)$ è sempre divisibile per $\nu(p-1)$.
Possiamo allora introdurre un altro quoziente

$$\omega(p) = \frac{\eta(p)}{\nu(p-1)} = \nu(p-1)^{-1} \bmod p$$

Ecco l'inizio della sequenza $\omega(p)$

$$1, 2, 3, 2, 1, 10, 7, 15, 20, 1, 14, 19, 11, 23, 6, 11, 45, 42, 37, 34, 10, 29, 76, 77, 14, 71, 12, 88, 40, 22, \cdots$$

Le sequenze $\eta(p), \omega(p)$ non sono in $OEIS$.
Nel prossimo paragrafo esaminiamo una generalizzazione del Teorema di Wilson, dovuta a Gauss.

6 TCR e Teorema di Gauss

Abbiamo visto in (3) che i coprimi con n sono tutti e soli gli invertibili modulo n. Chiamiamo $\mathbb{Z}_n^*$ l'insieme (dei resti) degli invertibili modulo n.

$$\mathbb{Z}_n^* = \{a \in \mathbb{N} : \quad 0 \leq a \leq n-1,\ (a,n) = 1\} \tag{12}$$

$\mathbb{Z}_n^*$ è un gruppo.
Per certi n questo gruppo è ciclico, esiste cioè un elemento g che lo genera.
Quando questo accade ogni elemento di $\mathbb{Z}_n^*$ è una potenza di g.
Per esempio $\mathbb{Z}_9^*$ è ciclico, generato da 2.
Infatti, se calcoliamo le potenze di 2 modulo 9,

$$2, 2^2, 2^3, 2^4, 2^5, 2^6$$

otteniamo, ordinatamente,

$$2, 4, 8, 7, 5, 1$$

Un g che genera $\mathbb{Z}_n^*$ si dice *radice primitiva* di n. Pertanto un intero n possiede una radice primitiva se e solo se il gruppo $\mathbb{Z}_n^*$ è ciclico.
Gauss determinò gli n che possiedono una radice primitiva.

Teorema 12. *n possiede una radice primitiva se e solo se*

- $n = 2, 4$
- $n = p^e$*, con p primo dispari*
- $n = 2p^e$*, con p primo dispari*

dove e è un un intero qualsiasi $e \geq 1$

Per abbreviare diciamo che n è RP se possiede una radice primitiva. Quindi 50 è RP, 8 non è RP.

Gauss generalizzò il Teorema di Wilson.
Introduciamo una notazione (non convenzionale) che generalizza il fattoriale

$$n! = \prod_{1 \leq k \leq n} k$$

Definiamo

$$n!_c = \prod_{1 \leq k \leq n,\,(k,n)=1} k$$

Pertanto $n!_c$ è il prodotto di tutti gli interi positivi minori di n che sono *coprimi* con n.
I termini iniziali della sequenza $n!_c$

$1, 1, 2, 3, 24, 5, 720, 105, 2240, 189, 3628800, 385, 479001600, 19305, 896896, 2027025, \cdots$

E' la A001783 in $OEIS$.
Ovviamente $n!_c$ divide $n!$. Pertanto possiamo fabbricare la successione

$$\frac{n!}{n!_c}$$

che è

$$1, 2, 3, 8, 5, 144, 7, 384, 162, 19200, 11, 1244160, 13, 4515840, 1458000, 10321920, 17, \cdots$$

Si noti che si ha

$$\frac{n!}{n!_c} = n$$

se e solo se $n = 1$ oppure n è primo.
E' la A066570 di $OEIS$.

Gauss generalizzò una parte del Teorema di Wilson.

Teorema 13.
Se n è RP allora

$$n!_c \equiv -1 \, mod \, n$$

Se n non è RP allora

$$n!_c \equiv 1 \, mod \, n$$

Per esempio, 8 non è RP e infatti

$$8!_c = 1 \times 3 \times 5 \times 7 = 105 \equiv 1 \bmod 8$$

Mentre 9 è RP e si ha

$$9!_c = 1 \times 2 \times 4 \times 5 \times 7 \times 8 \equiv 8 \bmod 9$$

(Si ricordi sempre che, modulo n, -1 è $n - 1$)

Utilizzando (13) possiamo definire una funzione $G(n)$, dove n è un intero maggiore di 0, detta *quoziente di Gauss*.

Definizione 14.
Se n è RP

$$G(n) = \frac{n!_c + 1}{n}$$

Se n non è RP

$$G(n) = \frac{n!_c - 1}{n}$$

Ecco la successione dei $G(n)$

$$0, 1, 1, 1, 5, 1, 103, 13, 249, 19, 329891, 32, 36846277, 1379, 59793, 126689, \cdots$$

A parte lo 0 iniziale, è la A157249 in $OEIS$.
Lo 0 all'inizio è dovuto al fatto che considero 1 non RP. La A157249 inizia invece con 2.

Ora facciamo entrare in campo il TCR.

Dato il sistema di due congruenze

$$\begin{cases} x \equiv a \bmod n \\ x \equiv b \bmod m \end{cases}$$

con n, m coprimi, sappiamo che ha una soluzione, unica modulo nm.
Denotiamo la soluzione con

$$\tau([a, b], [n, m])$$

Utilizzando (4) possiamo scriverla esplicitamente

$$\tau([a, b], [n, m]) = [(n^{-1} \bmod m)nb + (m^{-1} \bmod n)ma] \bmod (nm) \tag{13}$$

Naturalmente le soluzioni sono infinite, ma tutte differiscono dalla (13) per un multiplo di mn.

Utilizzeremo nel seguito una variante della $\nu(n)$, la funzione $\nu_c(n)$ uguale al minimo comune multiplo degli interi coprimi con n, compresi tra 1 e n.

La sequenza $\nu_c(n)$ è

$$1, 1, 2, 3, 12, 5, 60, 105, 280, 63, 2520, 385, 27720, 6435, \cdots$$

E' la A038610 in $OEIS$.

Ovviamente $\nu_c(n)$ divide $\nu(n)$.
La sequenza dei rapporti

$$\frac{\nu(n)}{\nu_c(n)}$$

è

$$1, 2, 3, 4, 5, 12, 7, 8, 9, 40, 11, 72, 13, 56, 45, 16, 17, 144, 19, 80, 63$$

E' la A064446 in $OEIS$

Supponiamo che n sia RP.
Per il Teorema (13) il numero $n!_c + 1$ soddisfa la

$$\begin{cases} x \equiv 0 \bmod n \\ x \equiv 1 \bmod \nu_c(n) \end{cases} \tag{14}$$

Utilizzando la (13) si vede che la soluzione minima di (14) è

$$\tau([0,1],[n,\nu_c(n)]) = (n^{-1} \bmod \nu_c(n))n$$

Supponiamo invece che n non sia RP.
Sempre per il Teorema (13) il numero $n!_c - 1$ soddisfa la

$$\begin{cases} x \equiv 0 \bmod n \\ x \equiv -1 \bmod \nu_c(n) \end{cases} \tag{15}$$

Ancora da (13) segue che la soluzione minima di (15) è

$$\tau([0,-1],[n,\nu_c(n)]) = (-n^{-1} \bmod \nu_c(n))n$$

Il caso $n = 1$ è singolare.
Il sistema diventa

$$\begin{cases} x \equiv 0 \bmod 1 \\ x \equiv -1 \bmod 1 \end{cases}$$

Modulo 1 tutti gli interi sono congruenti. La soluzione non negativa minima in questo caso è 0.
Questo conduce a definire un nuovo quoziente di Gauss $G_1(n)$

Definizione 15. Se n è RP

$$G_1(n) = \frac{\tau([0,1],[n,\nu_c(n)])}{n} = (n^{-1} \bmod \nu_c(n))$$

Se $n \neq 1$ non è RP

$$G_1(n) = \frac{\tau([0,1],[n,\nu_c(n)])}{n} = (-n^{-1} \bmod \nu_c(n))$$

$G_1(1) = 0$

La sequenza $G_1(n)$ comincia con

$$0, 1, 1, 5, 1, 43, 13, 249, 19, 2291, 32, 6397, 1379, 3737, 36599, 423953, 4727, \cdots$$

Non si trova in $OEIS$.
Infine, ragionando come nel paragrafo precedente, si vede che la funzione $\gamma(n)$ così definita

Definizione 16. Se n è RP

$$\gamma(n) = \frac{n!_c + 1 - (n^{-1} \bmod \nu_c(n))n}{n\nu_c(n)}$$

Se $n \neq 1$ non è RP

$$\gamma(n) = \frac{n!_c - 1 - (-n^{-1} \bmod \nu_c(n))n}{n\nu_c(n)}$$

$\gamma(1) = 0$

ha valori interi.

La sequenza $\gamma(n)$ è

$$0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 130, 0, 1329, 0, 7, 2, 1707670, 0, 27502484, 0, 609, 42, 209927657739, 0, \cdots$$

Anche questa successione non si trova in $OEIS$.

Gli zeri presenti nella successione $\gamma(n)$ stupiscono e possono trarre in inganno.
C'è uno zero per tutti e soli gli n tali che

$$G(n) = G_1(n)$$

Calcolando $\gamma(n)$ fino a $n = 6000$ ho trovato 0 soltanto per $n =$

$$1, 3, 4, 5, 6, 8, 9, 10, 12, 14, 18, 20, 24, 30, 42, 60$$

E' possibile che questi siano gli unici zeri della γ. Al crescere di n, $\gamma(n)$ aumenta in modo estremamente rapido. Per esempio, $\gamma(5987)$ ha 17412 cifre!
L'apparizione di uno 0, o anche di un numero piccolo, sembrerebbe un miracolo.

Esiste un 17° zero di γ?

Vengono detti *numeri di Wilson* gli interi n tali che il quoziente di Gauss $G(n)$ sia ancora divisibile per n. Dunque n è un numero di Wilson se e solo se

$$\frac{G(n)}{n}$$

è intero.

Ovviamente i primi di Wilson sono numeri di Wilson, perché, se p è primo

$$W(p) = G(p)$$

La sequenza dei numeri di Wilson è la A157250

$$1, 5, 13, 563, 5971, 558771, 1964215, 8121909, 12326713, 23025711, 26921605, 341569806, 399292158, \cdots$$

Come si è visto sopra, solo tre primi di Wilson sono noti

$$5, 13, 563$$

Pertanto gli interi dell'elenco, da 5971 in poi, sono composti.

Il primo numero di Wilson composto è stato trovato da Kloss nel 1975, tutti gli altri da T. Agoh, K. Dilcher, e L. Skula ([1]).

E' naturale allora cercare gli interi n tali che il quoziente

$$\frac{G_1(n)}{n}$$

sia intero. Chiamiamoli tcr numeri.

Poiché se p è primo

$$G_1(p) = W_1(p)$$

Abbiamo visto che $W_1(p)/p$ è intero per p=$2, 5, 31$. Questi sono quindi tcr numeri.

Cercando fino a $n = 10000$ ho trovato i seguenti tcr numeri

$$2, 5, 31, 1284, 4500, 5788$$

Naturalmente una ricerca di pura forza bruta diventa presto impossibile. Per trovare molti tcr numeri bisognerebbe restringere il campo delle possibilità, studiando le proprietà aritmetiche degli interi $G_1(n)$, in modo analogo a quanto è stato fatto in ([1]) per i $G(n)$.

7 Edificare il vuoto con grande merito

E' noto che nella sequenza dei numeri naturali esistono tratti privi di primi arbitrariamente lunghi. Diciamo *gap* tra primi la differenza di due primi consecutivi.

Sia $n \geq 4$ un intero positivo. Nella lista

$$n! - 2, n! - 3, \cdots, n! - n$$

ci sono $n - 1$ interi consecutivi composti.

Se n è dispari possiamo andare avanti di un passo. In questo caso nella lista

$$n! - 2, n! - 3, \cdots, n! - n - 1$$

ci sono n interi composti

Il bello è che sappiamo esattamente dove sono *a priori*, senza alcuna necessità di una osservazione. L'aspetto negativo è che, se vogliamo intervalli vuoti grandi, diventa difficile persino scrivere i numeri coinvolti.

Inoltre i gap associati a questi intervalli hanno un merito assai basso.

Dato un gap $p_n - p_{n-1}$ tra due primi consecutivi si definisce merito del gap il numero

$$\frac{p_n - p_{n-1}}{\log p_{n-1}}$$

Se abbiamo un intervallo I di interi composti consecutivi, ovviamente I è situato tra due primi consecutivi p_{n-1}, p_n. Possiamo allora parlare di merito associato all'intervallo.

Se desideriamo, per esempio, un vuoto di primi di lunghezza 11, utilizzando i fattoriali, dobbiamo partire da $11! - 2$, ottenendo

$$39916798, 39916797, 39916796, 39916795, \cdots, 39916791, 39916790, 39916789, 39916788$$

Questi 11 interi sono certamente composti. Abbiamo in un certo senso fabbricato noi questo vuoto. In genere però lo spazio ottenuto è più grande.

In questo caso, i primi a sinistra e a destra di I sono 39916787 e39916801. Il gap è 14, con merito 0.799.

Un miglioramento si può ottenere considerando, invece dei fattoriali, i cosiddetti primoriali.

Sia p un numero primo. Definiamo il primoriale

$$p\# \ = \ \text{prodotto di tutti i primi} \leq p$$

Questa è la sequenza dei primoriali $2\#$, $3\#$, ...

$$2, 6, 30, 210, 2310, 30030, 510510, 9699690, 223092870, 6469693230, \cdots$$

E' la A002110 di OEIS.

In ([9]) l'autore presenta un metodo per generare intervalli di interi composti, utilizzando il TCR. Vediamolo.

Denotiamo con p_n l'n-esimo primo. Per esempio $p_6 = 13$.

Poniamo $P_n = p_n\#$ e supponiamo $n > 1$, ovvero $P_n \neq 2$.

Allora sono tutti composti i numeri

$$P_n - 2, P_n - 3, \cdots, P_n - p_n, P_n - p_n - 1$$

$$P_n + 2, P_n + 3, \cdots, P_n + p_n, P_n + p_n + 1$$

Se utilizziamo il TCR, possiamo calcolare x tale che

$$\begin{cases} x \equiv -1 \bmod p_{n+2} \\ x \equiv 0 \bmod P_n \\ x \equiv 1 \bmod p_{n+1} \end{cases}$$

Poiché $x \equiv 0$ modulo P_n, x è divisibile per i primi $p_1 \dots p_n$ e quindi sono composti tutti gli interi

$$x, \quad x \pm k \quad \text{con} \quad 2 \leq k \leq p_n + 1$$

Inoltre dalla prima e dalla terza congruenza segue che p_{n+2} divide $x + 1$ e p_{n+1} divide $x - 1$.

Pertanto la sequenza

$$x - p_n - 1, x - pn, \cdots, x - 1, x, x + 1, \cdots, x + p_n, x + p_n + 1$$

e formata da interi composti consecutivi.

Abbiamo costruito un vuoto di lunghezza almeno $2p_n + 3$, al quale corrisponde un gap (differenza tra il primo a destra e quello a sinistra) di almeno $2p_n + 4$.

Quasi sempre l'ampiezza del vuoto che si osserva è maggiore.

Se prendiamo $n = 5$, e quindi $p_n = 11$ e $11\# = 2310$, applicando il metodo di Watson troviamo che la soluzione di

$$\begin{cases} x \equiv -1 \bmod 17 \\ x \equiv 0 \bmod 2310 \\ x \equiv 1 \bmod 13 \end{cases}$$

è $c = 217140$. Questo è il centro di un intervallo vuoto garantito di lunghezza $2 \times 11 + 3 = 25$. Vi sono 12 interi a sinistra di c e 12 alla sua destra.

Il primo alla sinistra di c è 217121, e quello alla sua destra è 217157. Abbiamo quindi trovato un intervallo vuoto di 35 interi e un gap uguale a 36. Il merito di questo gap è 2.92.

Possiamo studiare una piccola variante dell'idea di Watson. Invece di utilizzare p_{n+1} e p_{n+2}, possiamo, dati tre primi dispari p, q, r risolvere la

$$\begin{cases} x \equiv -1 \bmod q \\ x \equiv 0 \bmod p\# \\ x \equiv 1 \bmod r \end{cases} \tag{16}$$

Le sole condizioni, affinché il sistema abbia soluzioni, sono

$$r \neq q \quad q, r > p$$

La funzione centrale è la $C(p,q,r)$ che dà la soluzione x del sistema (16).
La C ha un andamento assai irregolare, ed è difficile prevedere quello che fa.
Per esempio calcolando $C(3,7,p_n)$ con $n \geq 5$ troviamo

$$342, 300, 426, 552, 300, 552, 342, 1518, 1518, 216, 48, 1644, 1476, 1770, 1140, 1350, \cdots$$

Se invece calcoliamo $C(3,p_n,7)$ con $n \geq 5$ troviamo

$$120, 246, 288, 246, 666, 666, 960, 36, 204, 1590, 1926, 582, 1002, 792, 1674, 1632, \cdots$$

Una cosa che sappiamo con certezza è

$$0 < C(p,q,r) < p\# \times q \times r$$

La seconda cosa che sappiamo è che $C(p,q,r)$ è un multiplo di $p\#$.

$$\exists k \quad C(p,q,r) = kp\#$$

Per costruzione q divide $x+1$. Se $q \neq x+1$ allora $x+1$ è composto. Seguono poi $x+2$, $x+3 \cdots$ fino a $x+p+1$ (in quanto $x+p+1$ è pari).

Così, guardando a sinistra, per costruzione r divide $x-1$. Se $r \neq x-1$ allora $x-1$ è composto. Seguono poi $x-2$, $x-3 \cdots$ fino a $x-p-1$.

Pertanto, se $q \neq x+1$ e $r \neq x-1$ abbiamo un vuoto di lunghezza $2p+3$.

A sinistra e destra del vuoto ci sono due primi, che denotiamo con $S(p,q,r)$ e $D(p,q,r)$.

Questi due primi determinano un gap

$$G(p,q,r) = D(p,q,r) - S(p,q,r)$$

e un merito

$$M(p,q,r) = \frac{G(p,q,r)}{\log S(p,q,r)}$$

Per p fissato, al variare di r e q l'intervallo si sposta in $\mathbb{N}$, perché cambia il k della soluzione $C(p,q,r) = kp\#$, e il gap varia, rimanendo sempre maggiore o uguale al suo minimo $2p+4$.

Tutto questo avviene sempre, tranne alcuni precisi casi particolari.

Questi casi sono

1. $x = q-1 \quad x \neq r+1$
2. $x = r+1 \quad x \neq q-1$

3. $x = q - 1 = r + 1$

Tutti questi casi si presentano.
Diciamo che la terna (p, q, r) è *speciale* di tipo i se verifica uno dei casi $i = 1, 2, 3$.

Teorema 17.
Dato p ci sono infinite terne speciali (p, q, r) di tipo 1 o di tipo 3.

Dimostrazione. Per un ben noto teorema dovuto a Dirichlet, nella successione

$$kp\# + 1$$

esistono infiniti primi.
Siano $k_1, k_2, \ldots$ i valori di k cui corrispondono primi.
Se $k_i p\# - 1$ è primo per tutti gli i tranne un numero finito, ci sono infinite terne di tipo 3.
Altrimenti esistono infiniti indici j tali che $k_j p\# - 1$ è composto.
Prendiamo uno di questi j. Sia r un fattore primo di $k_i p\# - 1$.
Allora la terna (p, q, r) è speciale di tipo 1. □

Allo stesso modo si può provare che

Teorema 18.
Dato p ci sono infinite terne speciali (p, q, r) di tipo 2 o di tipo 3.

Se si accetta la ipotesi di Schinzel, si può dimostrare che, per ogni p esistono infinite terne speciali di tipo 3.

Facciamo un esempio con $p = 13$.

Si ha $13\# = 30030$.
La sequenza dei k tali che $30030k + 1$ è primo è

$$4, 5, 6, 9, 10, 11, 13, 14, 15, 18, 20, 22, 28, 29, 31, 32, 35, 40, 41, 42, \cdots$$

Se prendiamo $k = 4$ abbiamo $q = 4 \times 30030 + 1 = 120121$.
Inoltre $4 \times 30030 - 1 = 113 \times 1063$.
Otteniamo allora due terne speciali di tipo 1, $(13, 120121, 113)$ e $(13, 120121, 1063)$. Per costruzione si ha

$$C(13, 120121, 113) = C(13, 120121, 1063) = 120120$$

Per $k = 6$ $q = 6 \times 30030 + 1 = 180181$.

Accade ora che $6 \times 30030 - 1 = 180179$ è primo.
Pertanto $(13, 180181, 180179)$ è una terna speciale di tipo 3.

Costruiamo adesso terne speciali di tipo 2.

Il più piccolo k tale che $k \times 30030 - 1$ è primo, è $k = 1$.
Fattorizzando 30031 si trova $30031 = 59 \times 509$.

Otteniamo così due terne speciali di tipo 2, $(13, 59, 30029)$ e $(13, 509, 30029)$. Per costruzione si ha

$$C(13, 59, 30029) = C(13, 509, 30029) = 30030$$

Il caso estremo di terne speciali di tipo 3 si ha quando $k = 1$.
In questo caso $r = p\# - 1$ e $q = p\# + 1$.
Diciamo singolare una terna (p, q, r) tale che siano verificate le condizioni appena dette.

Si ha dunque una terna singolare quando $p\#$ è in mezzo a due primi gemelli.
Questo fatto si verifica per

$$p = 3, p = 5, p = 11$$

Non sono noti altri casi, si veda in $OEIS$ la A088256.

Per ora quindi conosciamo soltanto tre terne singolari

$$(3, 7, 5),\ (5, 31, 29),\ (11, 2311, 2309)$$

Penso che sia estremamente difficile trovare altre terne singolari, se pur esistono.

Torniamo al caso generale. Supponiamo che le terne coinvolte non siano speciali.

La funzione C calcola $c = C(p, q, r)$ con una sola garanzia: c è composto e sia a destra che a sinistra di c ci sono $p+1$ interi composti. Spesso però ce ne sono di più. Introduciamo allora quella che chiamo *amplificazione*, $A(p, q, r)$.

$$A(p, q, r) = \frac{G(p, q, r)}{2p + 4}$$

L'amplificazione è dunque il rapporto tra il gap relativo all'intervallo vuoto cui $C(p, q, r)$ appartiene e la lunghezza $(+1)$ dell'intervallo vuoto garantito.
Ovviamente

$$A(p, q, r) \geq 1$$

Quando l'amplificazione è 1 non abbiamo guadagnato nulla, non siamo andati oltre all'ampiezza garantita.

Poiché (p, q, r) non è speciale, quando $A(p, q, r) = 1$, $C(p, q, r)$ si trova esattamente al centro dell'intervallo. Cioè

$$A(p, q, r) = 1 \quad \Rightarrow \quad C(p, q, r) = \frac{D(p, q, r) + S(p, q, r)}{2}$$

Non vale però il viceversa. Facciamo un esempio.

Se calcoliamo la sequenza dei p_n, con $n \geq 5$, dei primi tali che

$$C(5,7,p_n) = \frac{D(5,7,p_n) + S(5,7,p_n)}{2}$$

troviamo

$$13, 17, 23, 41, 53, 67, 73, 79, 83, 97, 107, 131, 137, 149, 157, 163, 181, 197, \cdots$$

Se invece calcoliamo la sequenza dei p_n, con $n \geq 5$, dei primi tali che

$$A(5,7,p_n) = 1$$

troviamo una sottosequenza propria (strettamente contenuta)

$$13, 23, 53, 73, 83, 131, 137, 157, 163, 197, 211, 229, 233, 257, 271, 281, 367, \cdots$$

Per esempio, dato $r = 17$ abbiamo
$S(5,7,17) = 1129$
$D(5,7,17) = 1151$
$G(5,7,17) = 22 > 2 \times 5 + 4 = 14$
$A(5,7,17) = 1.571 > 1$
$C(5,7,17) = 1140 = \frac{1129+1151}{2}$

Pertanto $C(5,7,17)$ è nel centro dell'intervallo, ma l'amplificazione è diversa da 1, infatti è maggiore di 3/2.

La funzione $C(p,q,r)$ è in effetti molto interessante. Tra l'altro consente di definire in modo deterministico e sensato particolari sequenze di primi.

Quali sono i primi p tali che, almeno per una coppia di primi q, r $A(p,q,r) = 1$? Chiamiamo questi primi di classe $A1$.
Esiste una caratterizzazione

Teorema 19.
Un primo p è di classe $A1$ se e solo se esistono due primi q, r tali che, posto

$$c = C(p,q,r)$$

si ha

1. *c-1 non è primo*
2. *c+1 non è primo*
3. *c-p-2 è primo*
4. *c+p+2 è primo*

Dimostrazione. Le condizioni $1, 2$ assicurano che la terna (p, q, r) non è speciale.
Le condizioni $3, 4$ fanno sì che la lunghezza dell'intervallo vuoto, di centro c e raggio $p+1$, sia esattamente $2p + 3$. □

Questa caratterizzazione ha due conseguenze assai interessanti

Teorema 20. *Se p è di classe $A1$ allora p è il primo elemento di una coppia di primi gemelli.*

Dimostrazione. Se $p + 2$ non è primo, allora ha un fattore primo g minore di p.
Poiché g è un primo minore di p, g divide $c = kp\#$.
Pertanto $c + p + 2$ e $c - p - 2$ non possono essere primi, e p non è di classe $A1$. □

Corollario 21. *Se esistono infiniti primi di classe $A1$ allora esistono infiniti primi gemelli.*

Sorge quindi inevitabilmente la domanda:

Esisono numeri primi che sono il primo elemento di una coppia di gemelli e non sono di classe $A1$?

Per ora ho fatto soltanto una piccola ricerca, fornendo un certificato per tutti i primi gemelli minori di 1000.

Questi i primi coinvolti

3, 5, 11, 17, 29, 41, 59, 71, 101, 107, 137, 149, 179, 191, 197, 227, 239, 269, 281, 311, 347, 419, 431, 461, 521, 569, 599, 617, 641, 659, 809, 821, 827, 857, 881

E' l'inizio della sequenza A001359 in $OEIS$.

Per ogni primo p in questo elenco, ho calcolato $A(p, p + 2, p_n)$ fino a trovare p_n tale che $A(p, p + 2, p_n) = 1$. Diciamo che p_n è un testimone per p.

Questo è l'elenco dei 35 testimoni

11, 13, 67, 23, 167, 331, 499, 139, 131, 1867, 277, 2543, 4547, 14083, 2087, 521, 929, 547, 1787, 27073, 3833, 20599, 6353, 6427, 29863, 4349, 19301, 21419, 42379, 14827, 1499, 40519, 18671, 58439, 96479

Per esempio abbiamo

$A(17, 19, 23) = 1$
$A(857, 859, 59439) = 1$

In realtà i testimoni sono due, è la coppia (q, r) che testimonia per p. In questa esplorazione ho scelto q uguale al secondo elemento della coppia di gemelli.
Sono possibili altre soluzioni.

Prendiamo $p = 857$. Allora sono testimoni non solo $(859, 58439)$, ma anche $(5879, 74411)$. Cioè si ha
$A(857, 5879, 74411) = 1$

Le coppie di testimoni per un certo p sono in numero finito?

Veniamo ora al merito.

Il merito dei gap è assai importante, perché questo parametro permette di valutare la grandezza di un gap tenendo conto della grandezza dei primi coinvolti.

Incredibilmente una della varie forme di denaro digitale, Gapcoin, si basa proprio sulla ricerca di gap di grande merito!

A forza di scavare per estrarre il loro oro, i cercatori di Gapcoin sono arrivati intorno ai meriti più grandi attualmente noti.

I i primi 20 campioni di merito sono elencati nella pagina The Top-20 Prime Gaps.
I massimi meriti sono elencati dal più piccolo al più grande.
Si nota che il numero 13, 33.3228, è stato trovato da Gapcoin.
I Gapcoinisti sostengono che prossimamente tutti i record saranno loro. Può essere, almeno per quanto riguarda l'enorme potenza di calcolo impiegata.

La funzione $C(p, q, r)$ non è stata pensata per trovare grandi meriti.

Però guardavo ieri il campione dei campioni, il numero 20.
Si tratta dell'intervallo di estremi

$$3750992529339978877 - 3750992529339980293$$

Ha un gap uguale a 1416 e merito 33.108.
Ci ho pensato qualche minuto è ho visto che

$$c = C(7, 45442902289, 220646619372939937) = 3750992529339978930$$

Poiché c è compreso tra gli estremi, il gioco è fatto!
Abbiamo

$S(7, 45442902289, 220646619372939937) = 3750992529339978877$
$D(7, 45442902289, 220646619372939937) = 3750992529339980293$
$G(7, 45442902289, 220646619372939937) = 1416$
$M(7, 45442902289, 220646619372939937) = 33.108$
Si ottiene inoltre una amplificazione elevata
$A(7, 45442902289, 220646619372939937) = 78.666$

La pagina dei campioni non è del tutto aggiornata.

Nella pagina di Nyman e Nicely, si trova l'intervallo

$$1425172824437699411 - 1425172824437700887$$

Ha un gap uguale a 1476 e merito 35.310.
Ora si ha che

$$c = C(5, 203596117776814303, 385077769369819) = 1425172824437700120$$

Visto che c è nell'intervallo, tutti i valori corrisponderanno.

Infatti abbiamo
$S(5, 203596117776814303, 385077769369819) = 1425172824437699411$
$D(5, 203596117776814303, 385077769369819) = 1425172824437700887$
$G(5, 203596117776814303, 385077769369819) = 1476$
$M(5, 203596117776814303, 385077769369819) = 35.310$

Inoltre l'amplificazione è 105.429.

Questi intervalli si trovano con molti valori diversi di p, q, r.

In generale il problema è questo. Dati due primi consecutivi p_n, p_{n+1}, determinare tre primi p, q, r tali che

$$p_n < C(p, q, r) < p_{n+1}$$

.

Sono certo che i lettori attenti hanno capito come fare.

Nell'Appendice ho inserito il codice (in pari/gp) delle funzioni principali utilizzate in questa sezione.

Buona ricerca a tutti!

Riferimenti bibliografici

[1] T. Agoh, K. Dilcher, and L. Skula, Wilson quotients for composite moduli
Math. Comp. 67 (1998), pp. 843-861

[2] Manuel Blum, Coin flipping by telephone,
Proceedings of IEEE Spring Computer Conference, (1982) pp.133-137

[3] Albrecht Heeffer, Regiomontanus and Chinese Mathematics,
Philosophica 82 (2008), pp. 87-114

[4] Alessandro Languasco - Alessandro Zaccagnini, Introduzione alla Crittografia
Hoepli 2004

[5] Shen Kangsheng, Historical Development of the Chinese Remainder Theorem
Archive for History of Exact Sciences, Vol. 38, No. 4 (1988), pp. 285-305

[6] Oystein Ore, The general Chinese Remainder Theorem,
The American Mathematical Montly, Vol. 59 (1952) pp.365-370

[7] Anjing Qu, Why Mathematics in Ancient China?
Research Institute for Mathematical Sciences Kokyu Proceedings, Vol. 1392 (2004), pp. 15-26

[8] Lawrence W. Swienciki: The ambitious Horse ancient Chinese mathematics problems
Key Curriculum Press, 2001

[9] Rex Watson, Runs of Composite Integers and the Chinese Remainder Theorem
The Mathematical Gazette, Vol. 78, No. 482 (Jul., 1994), pp. 167-172

8 Appendice

Le funzioni sono scritte in linguaggio gp, perché esso è estremamente potente, elegante e completamente gratuito.

E' possibile scaricare il programma qui.

Copiate il testo delle tre funzioni qui sotto:

```
{\\primorial
primorial(p)=my(r,k);
r=1;k=1;
while(prime(k)<=p,r=r*prime(k);k++);
r;
}
{\\centrale
centrale(p,q,r)=my(g);
g=primorial(p);
lift(chinese([Mod(-1,q),Mod(0,g),Mod(1,r)]));
}
{\\merito
merito(p,q,r)=my(u,v,pp);
u=centrale(p,q,r);
v=u-1;
pp=nextprime(u);
while(!ispseudoprime(v),v=v-2);
[v,pp,pp-v,(pp-v)/log(v),1.0*(pp-v)/(2*p+4)];
}
```

in un editor di testo. Salvate poi il file con il nome (per esempio) centrale.gp

Supponiamo che centrale.gp sia sul disco c : nella directory

```
c:\pippo
```

Cliccate due volte sulla icona PARI apparsa sul desktop dopo la installazione.
Apparirà una finestra DOS simile a questa

```
Reading GPRC: gprc.txt ...Done.

GP/PARI CALCULATOR Version 2.7.1 (released)
i686 running mingw (ix86/GMP-5.1.3 kernel) 32-bit version
compiled: May 16 2014, gcc version 4.6.3 (GCC)
threading engine: single
(readline v6.2 enabled, extended help enabled)

Copyright (C) 2000-2014 The PARI Group

PARI/GP is free software, covered by the GNU General Public License, and comes
WITHOUT ANY WARRANTY WHATSOEVER.

Type ? for help, \q to quit.
Type ?12 for how to get moral (and possibly technical) support.

parisize = 4000000, primelimit = 500000
(16:56) gp >
```

Al prompt > scrivete

```
\r c:\pippo\centrale.gp
```

Potete ora utilizzare le funzioni.

Scrivete

```
vector(20,k,primorial(prime(k)))
```

Comparirà la parte iniziale della sequenza A002110 in $OEIS$.

La funzione centrale è la $C(p,q,r)$ che abbiamo visto insieme.

Provate centrale

```
centrale(5, 203596117776814303, 385077769369819)
```

Otterrete

$$1425172824437700120$$

La funzione *merito* riceve la terna di numeri primi p, q, r, dove q ed r sono diversi e maggiori di p.

Restituisce 5 numeri

1. S(p,q,r)
2. D(p,q,r)
3. G(p,q,r)
4. M(p,q,r)
5. A(p,q,r)

Provate

```
merito(5, 203596117776814303, 385077769369819)
```

Troverete il famoso gap uguale a 1476 con merito maggiore di 35 e amplificazione maggiore di 105.

Proviamo ora

```
merito(1607,1609,1515541)
```

Bisogna aspettare alcuni secondi (15 sul mio portatile).

Osservate che l'ultima componente, la quinta, del vettore risposta è 1. Questo prova che anche 1607 (primo elemento della coppia di gemelli $1607, 1609$) ha classe $A1$.

Infine consiglio a tutti l'eccellente testo ([4]).

Esso contiene le basi fondamentali della aritmetica modulare, dei campi finiti, dei numeri primi, una introduzione a pari/gp, e tante altre bellissime cose!