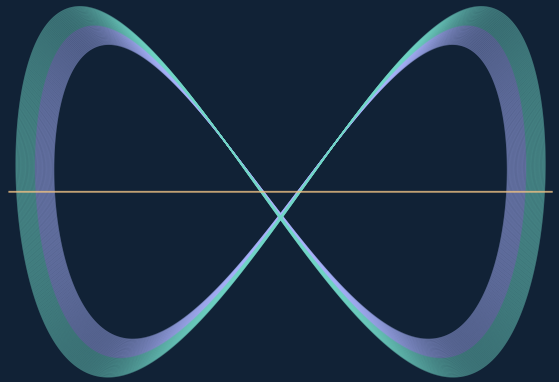
CALCOLO QUANTISTICO

L’algoritmo di Shor

Aritmetica, RSA e trasformata di Fourier



Una lettura con esempi numerici e richiami alle definizioni

Indice dei capitoli (1/2)

Titoli e numeri di pagina sono cliccabili. I segnalibri elencano capitoli e singole slide.
Il collegamento Indice, presente su ogni pagina, permette di tornare qui.

01 Il problema di Shor 4–14
Il precedente di Simon e la ricerca di un periodo

02 Divisori e coprimalità 15–33
Il massimo comun divisore e l'algoritmo di Euclide

03 Congruenze e inversi 34–56
Il calcolo con i resti e le operazioni reversibili

04 Potenze e ordine 57–81
Le ripetizioni delle potenze modulari

05 La costruzione di RSA 82–114
Chiavi, cifratura e correttezza della decifrazione

06 Il periodo del cifrato 115–127
Un esponente sufficiente a recuperare il messaggio

Indice dei capitoli (2/2)

Titoli e numeri di pagina sono cliccabili. I segnalibri elencano capitoli e singole slide.
Il collegamento Indice, presente su ogni pagina, permette di tornare qui.

07 La difficoltà della ricerca 128–136
Valutare una potenza e determinare il suo periodo

08 La rappresentazione di Fourier 137–151
Oscillazioni, campioni e frequenze

09 La ricerca quantistica del periodo 152–168
Ampiezze periodiche e interferenza

10 Dalla misura al messaggio 169–184
Approssimazioni razionali e decifrazione

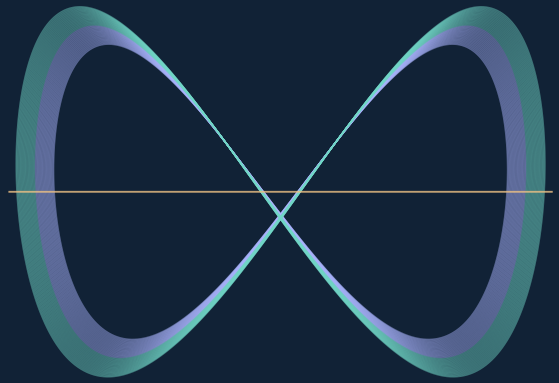
11 La realizzazione del circuito 185–200
Porte, aritmetica reversibile e misura

A Approfondimenti facoltativi 201–206
Il periodo e la fattorizzazione

Riferimenti bibliografici 207–208

CAPITOLO 01

Il problema di Shor



Il precedente di Simon
e la ricerca di un periodo

L’algoritmo di Shor

Il problema della fattorizzazione

Moltiplicando 3 per 5 otteniamo 15. La fattorizzazione percorre la domanda in senso opposto: dato 15, cerca numeri interi maggiori di 1 il cui prodotto sia 15. Per numeri così piccoli possiamo riconoscere il risultato a vista. Quando il numero contiene molte cifre, questa osservazione non fornisce più un metodo praticabile.

Indicheremo con N il numero da fattorizzare. L'algoritmo di Shor usa un calcolatore quantistico per cercare il periodo di una funzione costruita a partire da N. Questa ricerca permette anche di decifrare direttamente un messaggio RSA, senza ricavare prima i fattori del modulo. Seguiremo anzitutto tale percorso, dopo aver introdotto gli strumenti aritmetici necessari. Il collegamento fra periodo e fattorizzazione verrà ripreso nell'approfondimento conclusivo.

$$15 = 3 \cdot 5, \qquad 21 = 3 \cdot 7$$

Richiami Fattorizzare N significa trovare interi maggiori di 1 il cui prodotto sia N.

La lunghezza dell'ingresso

Per valutare il costo di un algoritmo dobbiamo precisare quanto è grande il suo ingresso. Un intero viene rappresentato da una sequenza di cifre. In un calcolatore queste cifre sono bit, ciascuno uguale a 0 oppure a 1. Il numero 21, per esempio, si scrive 10101_2 e richiede cinque bit.

Con cinque bit possiamo rappresentare tutti gli interi da 0 a 31. Aggiungendo un bit raddoppiamo il numero dei valori rappresentabili. Per questo un procedimento che prova un numero di candidati proporzionale a N può richiedere un numero di operazioni esponenziale nella lunghezza dell'ingresso. La distinzione fra valore numerico e numero di bit sarà essenziale nella discussione del costo di Shor.

$$21 = 16 + 4 + 1 = 10101_2$$

$$2^{n-1} \leq N < 2^n \quad \text{per un intero positivo di } n \text{ bit}$$

Richiami Un bit assume i valori 0 e 1. Con n bit si rappresentano 2^n valori distinti.

Verificare un risultato e trovarlo

Se qualcuno propone 3 e 7 come fattori di 21, basta eseguire il prodotto per controllare la risposta. Trovare quei fattori, quando non li conosciamo, è un compito diverso. La divisione per tentativi offre un metodo elementare, ma il numero di prove può diventare molto grande rispetto al numero di cifre di N.

Esistono algoritmi classici assai migliori della divisione per tentativi. Il vantaggio di Shor va confrontato con questi metodi, senza dedurne che la fattorizzazione classica sia stata dimostrata impossibile in tempo polinomiale. Il risultato di Shor è una procedura quantistica il cui costo cresce come una potenza della lunghezza dell'ingresso, con ripetizioni che permettono di controllare la probabilità di insuccesso.

Richiami La dimensione dell'ingresso è il numero di bit di N, non il valore di N.

La ripetizione dei valori di una funzione

Consideriamo una funzione che, agli ingressi $0, 1, 2, 3, 4, 5, \ldots$, associa i valori $A, B, C, A, B, C, \ldots$. Dopo tre passi la sequenza ricomincia. Diciamo che 3 è un periodo della funzione, perché spostare l'ingresso di tre unità lascia invariato il valore ottenuto.

Indichiamo la funzione con f e un suo periodo con r. Anche uno spostamento di sei unità conserva i valori. Quando occorre distinguere il primo ritorno dagli altri, parliamo di periodo minimo: il più piccolo spostamento positivo che riproduce tutta la sequenza. Shor riduce un problema aritmetico alla ricerca di un periodo di questo tipo. Gli esempi iniziali saranno piccoli, così da controllare a mano ciò che il procedimento quantistico dovrà ricostruire.

x	**0**	**1**	**2**	**3**
Valore	A	B	C	A

$$f(x + r) = f(x)$$

L'ingresso 3 riprende il valore dell'ingresso 0. La stessa ripetizione deve valere anche per tutti gli altri ingressi.

Richiami Un periodo $r > 0$ è uno spostamento dell'ingresso che lascia invariata la funzione.

Lo XOR fra stringhe binarie

Il problema di Simon, studiato prima di Shor, usa una diversa operazione sugli ingressi. Lo XOR confronta due stringhe bit per bit: produce 0 quando i due bit coincidono e 1 quando sono diversi. Non si eseguono riporti fra posizioni adiacenti, come accadrebbe nella somma ordinaria.

Per calcolare $001 \oplus 101$, confrontiamo prima i bit a sinistra, poi quelli centrali e infine quelli a destra. Otteniamo rispettivamente 1, 0 e 0, dunque il risultato è 100. Applicando una seconda volta lo XOR con 101 torniamo a 001. Ogni bit che la prima applicazione aveva invertito torna infatti al suo valore iniziale.

u	v	$u \oplus v$
0	0	0
0	1	1
1	0	1
1	1	0

$001 \oplus 101 = 100,$ $100 \oplus 101 = 001$

Richiami Lo XOR vale 1 fra bit diversi e 0 fra bit uguali. Non usa riporti.

Le coppie del problema di Simon

Nel problema di Simon esiste una stringa non nulla s, sconosciuta, che collega gli ingressi aventi lo stesso valore della funzione. La promessa del problema afferma che le coincidenze si verificano esattamente fra x e $x \oplus s$. Ogni valore della funzione individua quindi una coppia di ingressi.

Con $s = 101$, gli ingressi 001 e 100 appartengono alla stessa coppia. Anche 000 e 101 condividono un valore, ma quel valore è diverso da quello della prima coppia. Nel disegno le etichette dei risultati sono arbitrarie: interessa la struttura delle coincidenze. Se conoscessimo una coppia distinta x, y con lo stesso risultato, lo XOR $x \oplus y$ rivelerebbe direttamente s.

Stringa nascosta $s = 101$

x		y	$f(x) = f(y)$
000	———	101	A
001	———	100	B
010	———	111	C
011	———	110	D

In ogni riga: $y = x \oplus 101$ e $f(x) = f(y)$.

$$f(x) = f(x \oplus s), \qquad s \neq 0$$

Le otto stringhe di tre bit formano quattro coppie. Due ingressi nella stessa coppia hanno lo stesso valore della funzione.

Richiami $x \oplus s$ applicato due volte restituisce x. In Simon si assume $s \neq 0$.

L'informazione ottenuta da Simon

La procedura quantistica di Simon restituisce stringhe y che soddisfano un vincolo sulla stringa nascosta. Per interpretarlo bastano prodotti e somme di bit. Si moltiplicano i bit nelle posizioni corrispondenti di s e y, quindi si sommano i risultati. La somma deve essere pari, cioè avere resto 0 nella divisione per 2.

Scrivendo $s = s_2 s_1 s_0$, il risultato $y = 010$ impone che il bit centrale s_1 sia 0. Un risultato diverso può fornire un'altra condizione. Qui richiamiamo il tipo di informazione prodotto dall'algoritmo. Nella parte quantistica della lezione riprenderemo il meccanismo di interferenza che permette di selezionare risultati compatibili con una periodicità nascosta.

$$s_2 y_2 + s_1 y_1 + s_0 y_0 \equiv 0 \pmod 2$$

$$y = 010 \quad \Longrightarrow \quad s_1 = 0$$

Richiami Il resto modulo 2 è 0 per un numero pari e 1 per un numero dispari.

Due vincoli e una stringa nascosta

Supponiamo di aver ottenuto i risultati 010 e 101. Il primo fissa a 0 il bit centrale di s. Il secondo richiede che $s_2 + s_0$ sia pari. Poiché ciascun bit vale 0 oppure 1, i bit esterni devono essere uguali: sono entrambi 0 oppure entrambi 1.

Le stringhe rimaste sono quindi 000 e 101. La promessa di Simon esclude la stringa nulla, perciò in questo esempio ricostruiamo $s = 101$. Il punto utile per Shor è la divisione del lavoro. Il circuito produce campioni vincolati dalla struttura della funzione, mentre il calcolo classico combina i vincoli. Un singolo campione, come 010, non determinava ancora una risposta unica.

$$y^{(1)} = 010 : \; s_1 = 0$$

$$y^{(2)} = 101 : \; s_2 = s_0$$

$$s \in \{000, 101\}, \quad s \neq 000 \quad \Longrightarrow \quad s = 101$$

Richiami In Simon ogni campione impone una somma pari di prodotti di bit. La stringa nascosta è non nulla.

XOR e spostamento di un intero

La periodicità di Simon usa lo XOR, che può modificare più posizioni senza produrre un normale incremento numerico. Per esempio $001 \oplus 101 = 100$, mentre la somma ordinaria di 1 e 5 vale 6. Le due operazioni hanno dunque regole diverse anche quando usano le stesse rappresentazioni binarie.

Nella ricerca del periodo impiegata da Shor, gli ingressi equivalenti sono invece separati da uno stesso numero di passi: x, $x + r$, $x + 2r$ e così via. Per riconoscere questa struttura servirà una trasformata adatta all'addizione ordinaria. La trasformata di Fourier quantistica verrà introdotta attraverso esempi numerici, dopo aver costruito la funzione aritmetica di cui cerchiamo il periodo.

$$001 \oplus 101 = 100, \qquad 1 + 5 = 6$$

$$x, \quad x + r, \quad x + 2r, \quad x + 3r$$

Richiami Il periodo additivo r è una distanza fra ingressi. Lo XOR confronta invece i singoli bit.

I numeri che accompagneranno la lezione

Useremo pochi esempi ricorrenti, assegnando a ciascuno un compito preciso. Il numero 15 permetterà di osservare un periodo breve e una trasformata con risultati esatti. Il numero 21 servirà negli esercizi sulle potenze modulari e sul calcolo mediante quadrati successivi.

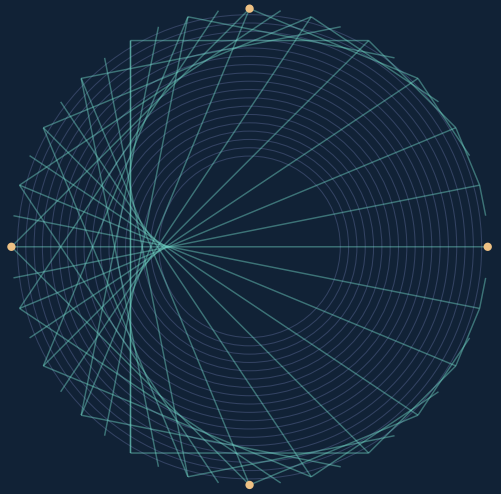
Per RSA useremo il prodotto $55 = 5 \cdot 11$. Lo stesso esempio accompagnerà la costruzione delle chiavi, la cifratura e il recupero del messaggio attraverso il periodo delle potenze del cifrato. Con questo modulo studieremo anche le approssimazioni che compaiono nella misura quantistica. Prima di questi sviluppi occorre rendere familiari divisori, coprimalità e resti. I richiami a fondo pagina riprenderanno le definizioni nel punto in cui servono, mentre gli esempi svolti mostreranno ogni operazione prima della sua forma generale.

Numero	Uso
15	Periodo breve e caso esatto
21	Potenze modulari e quadrati successivi
55	RSA e decifrazione mediante il periodo

Richiami Un periodo minimo è il più piccolo spostamento positivo che riproduce tutti i valori della funzione.

CAPITOLO 02

Divisori e coprimalità



Il massimo comun divisore e l’algoritmo di Euclide

L’algoritmo di Shor

Divisori e divisioni esatte

Dividendo 15 per 3 otteniamo 5 senza alcun resto. Per questo diciamo che 3 è un divisore di 15. La stessa informazione si può esprimere mediante un prodotto: $15 = 3 \cdot 5$. In questa lezione considereremo divisori positivi, quindi non includeremo i corrispondenti numeri negativi.

Il numero 4, invece, non divide 15: tre gruppi da quattro lasciano fuori tre unità. Per verificare che d sia un divisore di N cerchiamo dunque un intero q tale che $N = dq$. Scriviamo anche $d \mid N$, che si legge «d divide N». La barra verticale indica una relazione di divisibilità, non un'operazione di divisione.

$$15 = 3 \cdot 5, \qquad 3 \mid 15$$

$$15 = 4 \cdot 3 + 3, \qquad 4 \nmid 15$$

Richiami $d \mid N$ significa che esiste un intero q con $N = dq$.

I divisori compaiono in coppie

Quando troviamo un divisore d di N, il quoziente $q = N/d$ è a sua volta un divisore. Per 21, la divisione per 3 fornisce 7 e la divisione per 7 fornisce 3. La coppia descrive il medesimo prodotto, anche se scambiamo l'ordine dei fattori.

Ogni intero positivo ha almeno i divisori 1 e sé stesso. Questi divisori sono detti banali nel problema della fattorizzazione, perché il prodotto $N = 1 \cdot N$ è noto prima di qualsiasi ricerca. Un fattore non banale è invece un intero strettamente compreso fra 1 e N che divide N. Trovandone uno, otteniamo immediatamente il fattore complementare mediante una divisione esatta.

Divisore	Quoziente
1	21
3	7
7	3
21	1

$$21 = 1 \cdot 21 = 3 \cdot 7$$

Richiami Un fattore non banale d di N soddisfa $1 < d < N$ e $d \mid N$.

Numeri primi e numeri composti

Un intero maggiore di 1 è primo quando i suoi soli divisori positivi sono 1 e il numero stesso. Il numero 7 è primo: nessuno degli interi da 2 a 6 lo divide esattamente. Il numero 15 è composto, perché possiede anche i divisori 3 e 5.

Il numero 1 non rientra fra i primi. Questa convenzione permette di descrivere ogni intero maggiore di 1 come prodotto di primi senza aggiungere arbitrariamente fattori uguali a 1. Nell'algoritmo di Shor ci concentreremo su numeri composti. Se N è già primo, non esistono fattori non banali da cercare. Il riconoscimento dei primi è un problema distinto dalla fattorizzazione di un composto.

Intero	Divisori positivi	Tipo
7	1, 7	Primo
15	1, 3, 5, 15	Composto
1	1	Né primo né composto

Richiami Un primo ha esattamente due divisori positivi: 1 e sé stesso. Un composto ne possiede altri.

La scomposizione in fattori primi

Una prima divisione può lasciare un fattore ancora composto. Per esempio $36 = 4 \cdot 9$, ma sia 4 sia 9 si possono scomporre ulteriormente. Sostituendo $4 = 2 \cdot 2$ e $9 = 3 \cdot 3$ otteniamo un prodotto nel quale tutti i fattori sono primi.

Il risultato si scrive anche $36 = 2^2 \cdot 3^2$. L'esponente conta quante volte compare lo stesso fattore: 2^2 significa $2 \cdot 2$. La scomposizione in primi è unica, a meno dell'ordine dei fattori. Altri prodotti, come $6 \cdot 6$ o $3 \cdot 12$, conducono quindi agli stessi primi con le stesse ripetizioni. Questa proprietà spiega perché i divisori comuni possono essere letti confrontando i fattori primi dei numeri.

$$36 = 4 \cdot 9 = (2 \cdot 2)(3 \cdot 3) = 2^2 \cdot 3^2$$

Richiami a^k indica il prodotto di k fattori uguali ad a, per k intero positivo.

I divisori comuni di due interi

Cerchiamo ora i numeri che dividono contemporaneamente 12 e 18. Possiamo iniziare scrivendo i due elenchi di divisori. Nell'elenco di 12 compaiono 1, 2, 3, 4, 6 e 12. In quello di 18 compaiono 1, 2, 3, 6, 9 e 18.

I numeri presenti in entrambi gli elenchi sono i divisori comuni. In questo caso sono 1, 2, 3 e 6. Il più grande è 6. Questo confronto introduce il massimo comun divisore prima di qualunque algoritmo per calcolarlo. Il nome descrive esattamente il risultato richiesto: un divisore di entrambi i numeri, massimo fra tutti quelli che hanno questa proprietà.

Numero	Divisori
12	1, 2, 3, 4, 6, 12
18	1, 2, 3, 6, 9, 18
Comuni	1, 2, 3, 6

$$\gcd(12, 18) = 6$$

Richiami $\gcd(a, b)$, o MCD, indica il maggiore dei divisori positivi comuni di a e b.

Il MCD attraverso i fattori primi

La scomposizione in primi offre un secondo modo di comprendere il risultato precedente. Abbiamo $12 = 2^2 \cdot 3$ e $18 = 2 \cdot 3^2$. Un divisore comune può usare soltanto i fattori presenti in entrambi, senza ripeterli più volte di quanto permetta ciascun numero.

Possiamo quindi prendere un solo fattore 2 e un solo fattore 3. Il prodotto $2 \cdot 3 = 6$ è il massimo comun divisore. Un secondo 2 impedirebbe al risultato di dividere 18, mentre un secondo 3 impedirebbe di dividere 12. Questa lettura spiega il significato del MCD, ma non sarà il nostro metodo di calcolo principale: richiedere in anticipo le fattorizzazioni sarebbe scomodo proprio quando vogliamo trovarle.

$$12 = 2^2 \cdot 3, \qquad 18 = 2 \cdot 3^2$$

$$\gcd(12, 18) = 2 \cdot 3 = 6$$

Richiami Un divisore comune divide entrambi i numeri. Il MCD è il maggiore fra questi divisori.

Due numeri coprimi

I divisori positivi di 8 sono 1, 2, 4 e 8. Quelli di 15 sono 1, 3, 5 e 15. L'unico numero presente in entrambi gli elenchi è 1. Diciamo perciò che 8 e 15 sono coprimi, oppure primi fra loro.

La proprietà riguarda la coppia di numeri. Non afferma che ciascuno dei due sia primo: 8 e 15 sono entrambi composti. La definizione di coprimalità si esprime con $\gcd(8, 15) = 1$. Nel seguito questa condizione stabilirà quando una moltiplicazione modulare può essere invertita. Per il momento basta interpretarla come assenza di divisori comuni maggiori di 1, verificabile mediante il confronto dei due elenchi.

Divisori di 8	Divisori di 15
1	1
2	3
4	5
8	15

Comuni: 1
$\gcd(8, 15) = 1$

I divisori appartengono ai rispettivi elenchi. Il solo elemento comune è 1, quindi 8 e 15 sono coprimi.

Richiami a e N sono coprimi quando $\gcd(a, N) = 1$. Possono essere entrambi composti.

Un divisore comune maggiore di 1

Confrontiamo ora 6 e 15. I divisori di 6 sono 1, 2, 3 e 6, mentre quelli di 15 sono 1, 3, 5 e 15. Il numero 3 compare in entrambi gli elenchi e supera 1. La coppia non è dunque coprima.

Il risultato $\gcd(6, 15) = 3$ contiene già un'informazione utile per fattorizzare 15. Poiché 3 è strettamente compreso fra 1 e 15, è un fattore non banale. Il fattore complementare si ottiene dividendo: $15/3 = 5$. La versione di Shor destinata alla fattorizzazione comincia proprio con questo controllo classico del MCD. Alcune scelte della base possono rivelare un fattore prima di eseguire qualsiasi circuito quantistico.

$$\gcd(6, 15) = 3, \qquad 15 = 3 \cdot 5$$

Richiami Coprimi significa MCD uguale a 1. Un MCD d con $1 < d < N$ è già un fattore utile di N.

Quoziente e resto

Per calcolare il MCD senza fattorizzare i numeri useremo divisioni con resto. Dividendo 84 per 30, il multiplo di 30 più grande che non supera 84 è 60. Possiamo quindi formare due gruppi da 30 e restano 24 unità.

Il numero 2 è il quoziente e 24 è il resto. Il resto deve essere non negativo e minore del divisore: se fosse almeno 30, potremmo formare un altro gruppo. In generale, per $b > 0$, la divisione di $a \geq 0$ fornisce interi q, r tali che $a = qb + r$ e $0 \leq r < b$. Queste condizioni rendono unici quoziente e resto e permettono di ripetere ordinatamente il procedimento.

$$84 = 2 \cdot 30 + 24$$

$$a = qb + r, \qquad 0 \leq r < b$$

Richiami Nella divisione $a = qb + r$, q è il quoziente e r il resto. Il divisore b è positivo.

Sottrarre un multiplo conserva i divisori comuni

Supponiamo che un numero d divida sia 84 sia 30. Allora divide anche $2 \cdot 30$ e la differenza $84 - 2 \cdot 30 = 24$. Ogni divisore comune di 84 e 30 è quindi anche un divisore comune di 30 e 24.

Vale anche il ragionamento inverso. Se d divide 30 e 24, divide la loro combinazione $2 \cdot 30 + 24 = 84$. I divisori comuni delle due coppie coincidono, quindi coincide anche il loro massimo. Abbiamo sostituito la coppia $(84, 30)$ con $(30, 24)$, più piccola, senza cambiare la risposta. Questa proprietà fornisce il passaggio fondamentale dell'algoritmo di Euclide e spiega perché la sostituzione è lecita.

$$84 - 2 \cdot 30 = 24$$

$$\gcd(84, 30) = \gcd(30, 24)$$

Richiami Se d divide due interi, divide la loro somma, la loro differenza e ogni loro multiplo intero.

Le divisioni dell'algoritmo di Euclide

Ripetiamo ora la stessa sostituzione finché il resto diventa zero. Dalla coppia $(84, 30)$ otteniamo $(30, 24)$. Dividendo 30 per 24 rimane 6, quindi passiamo a $(24, 6)$. Infine 24 è un multiplo esatto di 6 e il resto è zero.

L'ultimo divisore usato è 6. La coppia $(24, 6)$ ha MCD uguale a 6, perché 6 divide entrambi i numeri e nessun divisore di 6 può essere maggiore di 6. Tutte le sostituzioni hanno conservato i divisori comuni, perciò anche la coppia iniziale ha MCD uguale a 6. Abbiamo ottenuto il risultato attraverso divisioni, senza conoscere le fattorizzazioni di 84 e 30.

$$84 = 2 \cdot 30 + 24$$

$$30 = 1 \cdot 24 + 6$$

$$24 = 4 \cdot 6 + 0$$

Richiami Euclide sostituisce (a, b) con (b, r), dove r è il resto della divisione di a per b.

La regola generale di Euclide

Il ragionamento svolto con 84 e 30 vale per qualsiasi divisione $a = qb + r$, con $b > 0$. Un divisore di a e b divide $r = a - qb$. Viceversa, un divisore di b e r divide $a = qb + r$. Le due coppie possiedono esattamente gli stessi divisori comuni.

La formula del MCD riassume questa equivalenza. Il vantaggio è che il nuovo resto soddisfa $0 \leq r < b$, quindi i numeri su cui prosegue il calcolo diminuiscono. Quando il resto è zero, il divisore corrente è la risposta. La proprietà conservata a ogni passaggio si chiama invariante dell'algoritmo: qui l'invariante è l'insieme dei divisori comuni e, di conseguenza, il suo massimo.

$$\gcd(a, b) = \gcd(b, r), \qquad a = qb + r$$

Richiami Nella divisione $a = qb + r$, il resto soddisfa $0 \leq r < b$. Euclide conserva il MCD a ogni sostituzione.

Il divisore dell'ultima divisione

Durante Euclide, ogni resto non nullo è un intero positivo minore del divisore che lo precede. Una successione di interi positivi strettamente decrescente non può proseguire indefinitamente. Prima o poi il resto diventa quindi zero e il procedimento termina.

Il MCD è il divisore usato nell'ultima divisione esatta. Per 84 e 30, i resti sono 24, 6 e 0, quindi il divisore finale 6 coincide con l'ultimo resto non nullo. Se invece partiamo da 12 e 6, la prima divisione è già esatta: $12 = 2 \cdot 6 + 0$. Non abbiamo prodotto alcun resto non nullo, ma il divisore 6 fornisce comunque il MCD. La formulazione attraverso il divisore finale comprende entrambi i casi.

$$\gcd(84, 30) = 6$$

$$12 = 2 \cdot 6 + 0, \qquad \gcd(12, 6) = 6$$

Richiami Euclide termina quando il resto è 0. Il divisore dell'ultima divisione è il MCD.

Riconoscere una coppia coprima

Consideriamo 40 e 3, numeri che torneranno nella costruzione delle chiavi RSA. La prima divisione fornisce $40 = 13 \cdot 3 + 1$. Dividendo poi 3 per 1 otteniamo resto zero. L'ultimo resto non nullo è dunque 1.

Concludiamo che $\gcd(40, 3) = 1$: i due numeri sono coprimi. Non abbiamo dovuto elencare i divisori di 40 né quelli di 3. Questo esempio è particolarmente breve perché il resto 1 compare subito. La divisione che lo produce avrà anche un secondo impiego: riscrivendola come $1 = 40 - 13 \cdot 3$, potremo trovare un inverso modulare. Per ora ci interessa il fatto che Euclide abbia certificato l'assenza di divisori comuni maggiori di 1.

$$40 = 13 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0$$

$$\gcd(40, 3) = 1$$

Richiami Due interi sono coprimi se il loro MCD è 1. Euclide calcola il MCD usando soltanto divisioni con resto.

Multipli comuni e minimo comune multiplo

Un multiplo di 6 si ottiene moltiplicando 6 per un intero: 6, 12, 18, 24 e così via. I multipli positivi di 8 iniziano invece con 8, 16 e 24. Il numero 24 compare in entrambi gli elenchi ed è il più piccolo valore positivo con questa proprietà.

Chiamiamo 24 minimo comune multiplo di 6 e 8, abbreviato mcm. Il MCD cerca un numero che divida entrambi gli ingressi, mentre il mcm cerca un numero divisibile per entrambi. Questa distinzione tornerà quando campioni diversi forniranno parti complementari del periodo. Un numero compatibile con entrambe le parti deve poter contenere un numero intero di ripetizioni di ciascuna.

Multipli di 6	Multipli di 8
6	8
12	16
18	24
24	32

$$\mathrm{mcm}(6, 8) = 24$$

Richiami Il mcm è il più piccolo intero positivo divisibile per entrambi i numeri. Il MCD divide invece entrambi.

Il primo multiplo comune di 2 e 3

Nel caso di 2 e 3, i multipli di 2 sono 2, 4, 6, 8 e così via. I multipli di 3 sono 3, 6, 9 e così via. Il primo valore comune è 6. Possiamo controllare il risultato con due divisioni: $6/2 = 3$ e $6/3 = 2$, entrambe senza resto.

Il numero 12 è anch'esso un multiplo comune, ma non è il minimo. Questo piccolo esempio anticipa una distinzione importante: un controllo può dimostrare che un numero possiede una proprietà senza dimostrare che sia il più piccolo a possederla. Nella ricerca dell'ordine incontreremo proprio questo problema. Conservare la parola «minimo» nella definizione impedisce di scambiare un risultato valido con quello cercato.

$$\operatorname{mcm}(2,3) = 6, \qquad \gcd(2,3) = 1$$

Richiami Il mcm richiede un minimo positivo. Un multiplo comune più grande continua a essere comune, ma non è il mcm.

Un controllo guidato su 14 e 21

Per verificare le definizioni, consideriamo la coppia 14 e 21. Vogliamo stabilire se i numeri sono coprimi e, se non lo sono, trovare il massimo comun divisore. Prima del calcolo, osserviamo che essere entrambi composti non basta a rispondere: anche 8 e 15 sono composti, ma sono coprimi.

Applichiamo Euclide partendo dal numero maggiore. La divisione di 21 per 14 lascia resto 7. La divisione di 14 per 7 è esatta, quindi il MCD è 7 e la coppia non è coprima. Possiamo controllare la conclusione mediante le scomposizioni $14 = 2 \cdot 7$ e $21 = 3 \cdot 7$. Il fattore comune 7 coincide con il risultato delle divisioni.

$$21 = 1 \cdot 14 + 7, \qquad 14 = 2 \cdot 7 + 0$$

$$\gcd(14, 21) = 7$$

Richiami La coprimalità riguarda una coppia: si verifica calcolando se il suo MCD è 1.

Un controllo guidato su 14 e 15

Consideriamo ora due interi consecutivi, 14 e 15. Il fatto che entrambi siano composti non basta a stabilire se abbiano divisori comuni maggiori di 1. Per rispondere dobbiamo confrontare i divisori oppure applicare l'algoritmo di Euclide alla nuova coppia.

La divisione $15 = 1 \cdot 14 + 1$ produce immediatamente resto 1, dunque il MCD è 1. Lo stesso risultato si comprende osservando la differenza: un divisore comune di 14 e 15 dovrebbe dividere anche $15 - 14 = 1$. L'unico divisore positivo di 1 è 1. Il ragionamento vale per qualunque coppia di interi positivi consecutivi, che risultano quindi sempre coprimi. L'esempio collega la definizione alla proprietà usata da Euclide.

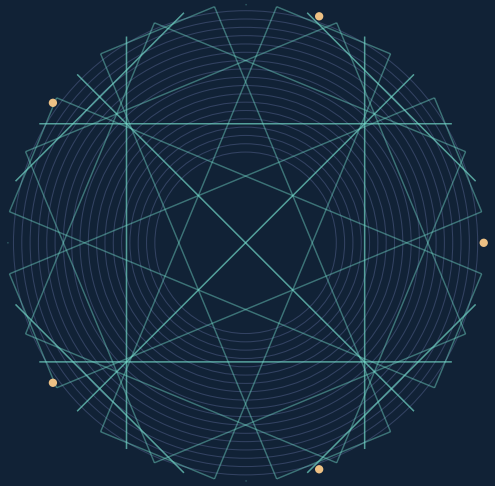
$$15 = 1 \cdot 14 + 1, \qquad \gcd(14, 15) = 1$$

Richiami Un divisore comune divide anche la differenza. Due interi positivi consecutivi hanno quindi MCD uguale a 1.

CAPITOLO 03

Congruenze e inversi

Il calcolo con i resti
e le operazioni reversibili



L’algoritmo di Shor

Interi con lo stesso resto

Dividiamo 17 e 7 per 5. Otteniamo $17 = 3 \cdot 5 + 2$ e $7 = 1 \cdot 5 + 2$. I quozienti sono diversi, ma il resto è lo stesso. Se ci interessa soltanto il resto nella divisione per 5, i due numeri forniscono dunque la medesima informazione.

Diciamo che 17 e 7 sono congruenti modulo 5 e scriviamo $17 \equiv 7 \pmod 5$. Anche 2 è congruente a entrambi, perché il suo resto è 2. Il simbolo di congruenza mantiene distinta questa relazione dall'uguaglianza ordinaria: 17, 7 e 2 sono interi diversi. L'aritmetica modulare permette di lavorare con il loro resto comune quando l'operazione successiva deve conservare solo quell'informazione.

$$17 = 3 \cdot 5 + 2, \qquad 7 = 1 \cdot 5 + 2$$

$$17 \equiv 7 \equiv 2 \pmod 5$$

Richiami $a \equiv b \pmod N$ significa che a e b hanno lo stesso resto nella divisione per N.

La congruenza attraverso la differenza

La differenza fra 17 e 7 è 10, cioè un multiplo di 5. Questo offre un secondo criterio per riconoscere la congruenza. Se due interi hanno lo stesso resto, possiamo scriverli come $a = qN + r$ e $b = pN + r$. Sottraendo, il resto scompare e otteniamo $a - b = (q - p)N$.

Viceversa, aggiungere o sottrarre un multiplo di N cambia il quoziente della divisione ma lascia invariato il resto. Le due definizioni sono quindi equivalenti. Useremo la lettura in termini di resti per eseguire calcoli e quella in termini di divisibilità per giustificare le formule. Il modulo N è sempre un intero positivo, che in questa lezione sarà maggiore di 1.

$$a \equiv b \pmod{N} \quad \Longleftrightarrow \quad N \mid (a - b)$$

$$17 - 7 = 10 = 2 \cdot 5$$

Richiami $N \mid (a - b)$ significa che la differenza fra a e b è un multiplo intero di N.

Un rappresentante fra 0 e N meno 1

Modulo 5, i possibili resti sono 0, 1, 2, 3 e 4. Tutti gli interi congruenti a 2 formano una stessa classe: vi appartengono, per esempio, -3, 2, 7, 12 e 17. La classe contiene infiniti interi, ma basta conservarne uno per descrivere il resto comune.

Sceglieremo normalmente il rappresentante non negativo minore di N. Per la classe precedente scegliamo dunque 2. La scrittura $a \bmod N$ indicherà proprio questo resto, quindi $17 \bmod 5 = 2$. La distinzione di notazione è utile: la congruenza mette in relazione due interi, mentre l'operazione di riduzione modulo N restituisce un particolare intero nell'intervallo da 0 a $N - 1$.

$$\ldots, -3, 2, 7, 12, 17, \ldots \quad \text{sono congruenti modulo } 5$$

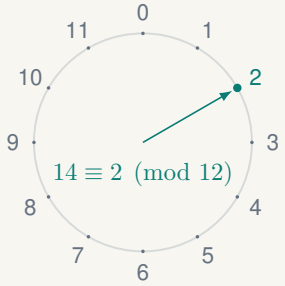
$$17 \bmod 5 = 2$$

Richiami $a \bmod N$ è il rappresentante con $0 \leq a \bmod N < N$. Una classe contiene tutti gli interi con quel resto.

Il ritorno dopo un giro completo

Un quadrante con dodici posizioni offre un'immagine concreta della riduzione modulo 12. Partendo da 0, dopo dodici passi torniamo a 0. Dopo altri due passi arriviamo alla posizione 2. Percorrere quattordici passi e percorrerne due conduce dunque alla stessa posizione.

La divisione $14 = 1 \cdot 12 + 2$ descrive lo stesso fatto: un giro completo e due passi restanti. Il disegno serve a visualizzare la ripetizione dei resti, ma non attribuisce alcun significato fisico speciale al modulo. In seguito useremo moduli come 15, 21 e 55. In tutti i casi un incremento di N lascia invariato il resto, anche quando non disegniamo un quadrante.



$14 = (1) \cdot 12 + 2$

Il giro completo corrisponde a dodici passi. La posizione finale dipende soltanto dai due passi che rimangono dopo il giro.

Richiami Aggiungere un multiplo di N lascia invariato il resto modulo N.

Ridurre gli addendi prima della somma

Vogliamo calcolare il resto di $17 + 9$ modulo 5. Possiamo prima eseguire la somma: $17 + 9 = 26$, che lascia resto 1. Possiamo anche ridurre separatamente gli addendi: 17 lascia resto 2 e 9 lascia resto 4. Sommando i resti otteniamo 6, che lascia nuovamente resto 1.

Il risultato coincide perché i multipli di 5 eliminati dai due addendi producono, sommati, ancora un multiplo di 5. Il calcolo modulare conserva dunque la somma dei resti, purché si riduca anche il risultato finale quando raggiunge o supera il modulo. Questa proprietà permette di sostituire numeri grandi con rappresentanti piccoli durante un calcolo, senza alterare il resto che vogliamo ottenere.

$$(17 + 9) \bmod 5 = 26 \bmod 5 = 1$$

$$(2 + 4) \bmod 5 = 6 \bmod 5 = 1$$

Richiami La riduzione modulo N conserva le somme: si possono ridurre gli addendi prima di sommarli.

Ridurre i fattori prima del prodotto

La stessa possibilità vale per i prodotti. Per trovare il resto di $17 \cdot 9$ modulo 5 possiamo calcolare $153 \bmod 5 = 3$. Riducendo prima i fattori, otteniamo invece $2 \cdot 4 = 8$, che lascia anch'esso resto 3. I numeri intermedi sono molto più piccoli.

Per capire la regola, scriviamo i fattori come multipli del modulo più i rispettivi resti. Sviluppando il prodotto, tutti i termini tranne il prodotto dei resti contengono un fattore N. Quei termini scompaiono quando consideriamo soltanto il resto. Questa osservazione giustifica le riduzioni intermedie nelle potenze modulari: dopo ogni moltiplicazione potremo ridurre il risultato, mantenendo il valore memorizzato fra 0 e $N - 1$.

$$17 \cdot 9 = 153 \equiv 3 \pmod 5$$

$$2 \cdot 4 = 8 \equiv 3 \pmod 5$$

Richiami Si possono ridurre modulo N i fattori e il prodotto finale senza modificare il resto.

I rappresentanti negativi

Anche un numero negativo appartiene a una classe di resti. Modulo 15, per esempio, -1 e 14 sono congruenti perché la loro differenza è 15. Scegliere -1 al posto di 14 può rendere più semplice un prodotto o una potenza, mentre 14 rimane il rappresentante non negativo convenzionale.

Un esempio che tornerà in RSA è -13 modulo 40. Aggiungendo 40 otteniamo 27, quindi i due numeri hanno lo stesso resto. Quando un calcolo produce un coefficiente negativo, questa operazione permette di convertirlo nel rappresentante fra 0 e 39. Il cambiamento riguarda la rappresentazione della classe, non la proprietà modulare che il numero soddisfa.

$$-1 \equiv 14 \pmod{15}$$

$$-13 + 40 = 27, \qquad -13 \equiv 27 \pmod{40}$$

Richiami Due interi sono congruenti modulo N se la loro differenza è un multiplo di N, anche se uno è negativo.

Una sequenza di riduzioni intermedie

Calcoliamo il resto di 8^3 modulo 15. Il prodotto ordinario vale 512, ma possiamo evitare di conservarlo per intero. Dopo la prima moltiplicazione otteniamo $8^2 = 64$, che lascia resto 4. Per la moltiplicazione successiva usiamo quindi 4 al posto di 64.

Il prodotto $4 \cdot 8 = 32$ lascia resto 2. La verifica diretta conferma il risultato, perché $512 = 34 \cdot 15 + 2$. Il vantaggio di ridurre dopo ogni prodotto diventerà importante per esponenti grandi. Questa pagina introduce soltanto la validità delle riduzioni intermedie. Nel capitolo sulle potenze costruiremo anche un metodo per diminuire il numero delle moltiplicazioni necessarie, sfruttando la scrittura binaria dell'esponente.

$$8^2 = 64 \equiv 4 \pmod{15}$$

$$8^3 \equiv 4 \cdot 8 = 32 \equiv 2 \pmod{15}$$

Richiami $8^3 = 8 \cdot 8 \cdot 8$. Ridurre un prodotto intermedio modulo N conserva il resto dei prodotti successivi.

Un prodotto che lascia resto 1

Cerchiamo un intero che, moltiplicato per 8, lasci resto 1 nella divisione per 15. Il numero 2 soddisfa la richiesta, perché $8 \cdot 2 = 16 = 15 + 1$. Diciamo che 2 è un inverso moltiplicativo di 8 modulo 15.

Il nome descrive la possibilità di annullare una moltiplicazione precedente. Se un numero x viene prima moltiplicato per 8 e poi per 2, il prodotto complessivo è $16x$. Modulo 15, $16x$ ha lo stesso resto di x, poiché $16x = x + 15x$. L'inverso modulare è un intero che soddisfa questa proprietà sui resti. Non coincide con la frazione ordinaria $1/8$, che appartiene a un diverso contesto di calcolo.

$$8 \cdot 2 = 16 \equiv 1 \pmod{15}$$

$$2(8x) \equiv x \pmod{15}$$

Richiami b è un inverso di a modulo N quando $ab \equiv 1 \pmod{N}$.

Recuperare il resto iniziale

Proviamo il ripristino con un ingresso preciso, $x = 7$. Moltiplicando per 8 otteniamo 56, il cui resto modulo 15 è 11. Se conserviamo soltanto 11, abbiamo perso il quoziente della divisione, ma possiamo ancora recuperare il resto iniziale mediante l'inverso 2.

Infatti $2 \cdot 11 = 22$, che lascia resto 7. Il calcolo torna all'ingresso iniziale perché $2 \cdot 8 \equiv 1 \pmod{15}$. Questa possibilità vale per tutti i resti, non soltanto per 7. È una proprietà della moltiplicazione per 8 nel modulo scelto. Cambiando moltiplicatore o modulo dovremo verificare nuovamente se esiste un inverso, senza assumere che ogni moltiplicazione modulare sia invertibile.

$$7 \xrightarrow{\times 8 \bmod 15} 11 \xrightarrow{\times 2 \bmod 15} 7$$

Richiami $8 \cdot 2 \equiv 1 \pmod{15}$: moltiplicare per 2 annulla sui resti la moltiplicazione per 8.

Una moltiplicazione senza inverso

Cerchiamo ora un inverso di 6 modulo 15. Dovremmo trovare interi b e k tali che $6b = 15k + 1$. Il membro sinistro è divisibile per 3. Anche $15k$ è divisibile per 3, mentre $15k + 1$ lascia resto 1 nella divisione per 3. L'uguaglianza è quindi impossibile.

La difficoltà dipende dal divisore comune 3 di 6 e 15. Qualunque prodotto $6b$ conserva quel fattore e non può differire da un multiplo di 15 esattamente di 1. Il confronto con 8 modulo 15 suggerisce una regola: la coprimalità rende possibile l'inverso. La dimostreremo usando le divisioni di Euclide, che producono anche un metodo concreto per calcolarlo.

$$6b \equiv 1 \pmod{15} \quad \Longleftrightarrow \quad 6b - 15k = 1$$

Richiami $\gcd(6, 15) = 3$. Un divisore comune di due interi divide anche ogni loro combinazione a coefficienti interi.

Rileggere una divisione di Euclide

Nel calcolo del MCD di 40 e 3 abbiamo ottenuto $40 = 13 \cdot 3 + 1$. Spostiamo il prodotto al secondo membro: $1 = 40 - 13 \cdot 3$. L'unità appare così come somma di multipli interi dei due numeri iniziali.

Consideriamo questa uguaglianza modulo 40. Il termine 40 ha resto zero e rimane $(-13) \cdot 3 \equiv 1 \pmod{40}$. Il coefficiente -13 è quindi un inverso di 3 modulo 40. Abbiamo ricavato l'inverso dalla stessa divisione che aveva dimostrato la coprimalità. La presenza del segno negativo non crea problemi: l'aritmetica modulare ammette rappresentanti negativi, che possiamo sostituire con un rappresentante non negativo della stessa classe.

$$40 = 13 \cdot 3 + 1 \quad \Longrightarrow \quad 1 = 40 - 13 \cdot 3$$

$$3(-13) \equiv 1 \pmod{40}$$

Richiami Un inverso di 3 modulo 40 è un intero d con $3d \equiv 1 \pmod{40}$.

L’inverso 27 modulo 40

Sostituiamo ora -13 con il rappresentante non negativo modulo 40. Aggiungendo 40 otteniamo 27. Poiché aggiungere un multiplo del modulo non cambia la classe, anche 27 deve essere un inverso di 3.

Possiamo verificare il risultato senza ripercorrere Euclide: $3 \cdot 27 = 81 = 2 \cdot 40 + 1$. Il resto è proprio 1. È utile separare la ricerca dalla verifica. Euclide ci ha fornito un candidato, mentre un singolo prodotto ne controlla la proprietà. Questa coppia di numeri comparirà in RSA come esponente pubblico ed esponente privato dell’esempio. Il modulo usato per scegliere gli esponenti sarà 40, distinto dal modulo 55 usato per trasformare i messaggi.

$$-13 + 40 = 27$$

$$3 \cdot 27 = 81 = 2 \cdot 40 + 1$$

Richiami $-13 \equiv 27 \pmod{40}$. Sostituire un fattore con un numero congruente conserva il resto del prodotto.

Risalire più divisioni

Un calcolo più lungo mostra come procedere quando il resto 1 non compare subito. Per 40 e 7, Euclide produce resti 5, 2 e 1. Partiamo dall'ultima divisione non esatta, che esprime 1 come $5 - 2 \cdot 2$, e sostituiamo a ritroso il resto 2 mediante la divisione precedente.

Otteniamo $1 = 5 - 2(7 - 5) = 3 \cdot 5 - 2 \cdot 7$. Sostituiamo infine $5 = 40 - 5 \cdot 7$. Il risultato è $1 = 3 \cdot 40 - 17 \cdot 7$. Modulo 40, il coefficiente -17 è quindi un inverso di 7. Il suo rappresentante non negativo è 23 e il controllo dà $7 \cdot 23 = 161 = 4 \cdot 40 + 1$. Ogni sostituzione usa soltanto una delle divisioni già eseguite.

$$40 = 5 \cdot 7 + 5, \quad 7 = 1 \cdot 5 + 2, \quad 5 = 2 \cdot 2 + 1$$

$$1 = 3 \cdot 40 - 17 \cdot 7$$

$$7 \cdot 23 = 161 \equiv 1 \pmod{40}$$

Richiami Risalire Euclide significa sostituire ogni resto con dividendo meno quoziente per divisore.

L'identità di Bézout

La risalita delle divisioni di Euclide consente sempre di scrivere il MCD come combinazione dei due numeri iniziali con coefficienti interi. Questa proprietà prende il nome di identità di Bézout. I coefficienti possono essere negativi, come negli esempi appena svolti.

Quando $\gcd(a, N) = 1$, otteniamo quindi interi u, v tali che $ua + vN = 1$. Considerando l'uguaglianza modulo N, il termine vN lascia resto zero. Rimane $ua \equiv 1 \pmod{N}$, perciò u è un inverso di a. Il procedimento che conserva le divisioni e ne ricava anche i coefficienti si chiama algoritmo di Euclide esteso. La parola «esteso» indica questa informazione aggiuntiva rispetto al solo MCD.

$$ua + vN = \gcd(a, N)$$

$$\gcd(a, N) = 1 \quad \Longrightarrow \quad ua \equiv 1 \pmod{N}$$

Richiami Bézout esprime il MCD come $ua + vN$ con u, v interi. Se il MCD è 1, u è un inverso modulo N.

La condizione esatta per avere un inverso

Abbiamo dimostrato che la coprimalità è sufficiente: quando il MCD di a e N vale 1, Euclide esteso produce un inverso. Dimostriamo anche che è necessaria. Se $ab \equiv 1 \pmod{N}$, esiste un intero k tale che $ab - kN = 1$.

Un divisore comune di a e N deve dividere sia ab sia kN, dunque anche la loro differenza 1. Può essere soltanto 1. L'esistenza di un inverso equivale quindi alla coprimalità. Questa equivalenza permette di verificare prima, con il MCD, se il problema di inversione ha una soluzione. Chiarisce anche perché il tentativo con 6 modulo 15 era impossibile, mentre quello con 8 riusciva.

$$a \text{ ha un inverso modulo } N \iff \gcd(a, N) = 1$$

Richiami $ab \equiv 1 \pmod{N}$ significa $ab - kN = 1$ per un intero k. Ogni divisore comune divide quella differenza.

Un insieme con un’operazione di gruppo

Nota facoltativa · Connessione algebrica

Riprendi il testo: p. 53

Un gruppo è un insieme G con un’operazione che combina due elementi e restituisce ancora un elemento di G. L’operazione è associativa: le parentesi non cambiano il risultato quando si combinano tre elementi. Esiste un elemento neutro, che lascia invariato ogni elemento. Ciascun elemento possiede inoltre un inverso, il cui prodotto con esso dà il neutro in entrambi gli ordini.

Nella moltiplicazione modulare il neutro è 1. La figura verifica alcune di queste proprietà modulo 15. Se anche scambiare i due fattori lascia invariato il prodotto, il gruppo si dice commutativo, o abeliano. Questo linguaggio riunisce le proprietà che permettono di annullare una moltiplicazione e di ricostruire l’ingresso.

Proprietà del prodotto modulo 15

Chiusura	$2 \cdot 7 \equiv 14$
Associatività	$(2 \cdot 4) \cdot 8 \equiv 2 \cdot (4 \cdot 8) \equiv 4$
Elemento neutro	$1 \cdot 7 = 7 \cdot 1 = 7$
Inverso di 2	$2 \cdot 8 \equiv 8 \cdot 2 \equiv 1$

Queste sono verifiche su elementi specifici.

Le uguaglianze mostrano il neutro, l’inverso e l’associatività in esempi modulo 15. Gli assiomi richiedono queste proprietà per tutti gli elementi del gruppo.

Richiami Un inverso di a modulo N soddisfa $ab \equiv 1 \pmod{N}$. Il neutro moltiplicativo è 1.

Il gruppo degli invertibili modulo 15

Nota facoltativa · Connessione algebrica

Riprendi il testo: p. 53

Una unità modulo N è un residuo che possiede un inverso moltiplicativo. Il criterio appena dimostrato identifica le unità con i residui coprimi con N. Il loro insieme si indica con $\mathbb{Z}_N^\times$. Il prodotto di due unità rimane invertibile: per annullarlo basta moltiplicare per gli inversi dei due fattori. Con il prodotto modulo N, questo insieme forma un gruppo abeliano.

Modulo 15 le unità sono $1, 2, 4, 7, 8, 11, 13, 14$. Il grafo accoppia ogni elemento con il suo inverso. Per esempio, $2 \cdot 8 \equiv 1$ e $7 \cdot 13 \equiv 1$. Il residuo 3 resta escluso, poiché ogni suo multiplo è divisibile per 3 e non può essere congruente a 1 modulo 15. Le potenze di una base coprima rimangono in questo gruppo, qualunque sia l'esponente intero non negativo.

Inversi in $\mathbb{Z}_{15}^\times$



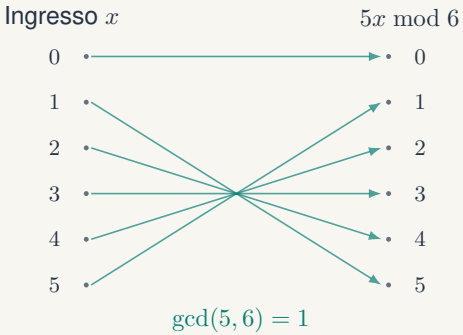
Ogni arco collega due inversi. Un cappio indica un elemento inverso di sé stesso. Il grafo rappresenta l'inversione, non tutti i prodotti possibili.

Richiami $\mathbb{Z}_N^\times$ contiene i residui a con $\gcd(a, N) = 1$. L'operazione è il prodotto modulo N.

Moltiplicare senza perdere un ingresso

Consideriamo tutti i resti modulo 6: 0, 1, 2, 3, 4 e 5. Moltiplicandoli per 5 e riducendo i prodotti modulo 6 otteniamo, nello stesso ordine, 0, 5, 4, 3, 2 e 1. Ogni resto compare una volta sola: la trasformazione ha riordinato l'elenco.

Un riordinamento senza perdite né ripetizioni si chiama permutazione. Qui possiamo annullarlo moltiplicando ancora per 5, perché $5 \cdot 5 = 25 \equiv 1 \pmod 6$. A ogni uscita corrisponde dunque un solo ingresso. Questa proprietà rende la moltiplicazione reversibile sul suo insieme di resti e prepara la costruzione dei circuiti modulari, che dovranno conservare la possibilità di risalire dagli stati finali agli stati iniziali.



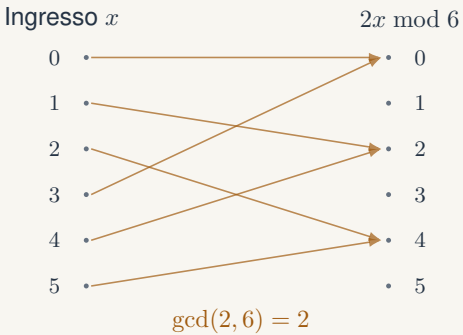
Ogni ingresso ha un'uscita e ogni uscita riceve una sola freccia. Moltiplicare nuovamente per 5 restituisce il resto iniziale.

Richiami Una permutazione riordina gli elementi senza perderli né ripeterli. $\gcd(5,6) = 1$ garantisce un inverso.

Ingressi distinti con la stessa uscita

Ripetiamo il confronto modulo 6 usando il moltiplicatore 2. Gli ingressi 0 e 3 producono entrambi resto 0. Gli ingressi 1 e 4 producono resto 2, mentre 2 e 5 producono resto 4. Restano soltanto tre uscite diverse.

Quando ingressi distinti condividono un'uscita parliamo di collisione. Se conosciamo soltanto l'uscita 2, non possiamo stabilire se l'ingresso fosse 1 oppure 4. La trasformazione non è una permutazione e non può essere annullata mediante una funzione della sola uscita. Il risultato concorda con il criterio aritmetico: $\gcd(2,6) = 2$, quindi 2 non possiede un inverso modulo 6. La coprimalità ha così una conseguenza concreta sulla conservazione dell'informazione.



$$2 \cdot 1 \equiv 2 \cdot 4 \equiv 2 \pmod 6$$

Più frecce arrivano alla stessa uscita. Conservare soltanto il resto finale non basta a ricostruire quale ingresso sia stato usato.

Richiami Una collisione associa la stessa uscita a ingressi diversi. Un moltiplicatore invertibile non può produrre collisioni.

La cancellazione richiede un inverso

Nell'aritmetica ordinaria cancelliamo spesso uno stesso fattore dai due membri di un'uguaglianza. Nelle congruenze occorre controllare una condizione aggiuntiva. Se $ax \equiv ay \pmod{N}$ e a possiede un inverso b, possiamo moltiplicare entrambi i membri per b. Poiché $ba \equiv 1$, otteniamo $x \equiv y$.

Senza inverso la conclusione può essere falsa. Modulo 6 abbiamo appena trovato $2 \cdot 1 \equiv 2 \cdot 4$, ma 1 e 4 non sono congruenti modulo 6. Il fattore 2 non può essere cancellato perché non è coprimo con 6. Richiameremo questa condizione quando dimostreremo che le potenze di una base coprima tornano a 1 e che il loro primo ritorno definisce un periodo.

$$ax \equiv ay \pmod{N}, \quad \gcd(a, N) = 1 \quad \Longrightarrow \quad x \equiv y \pmod{N}$$

Richiami Un fattore si può cancellare modulo N se è coprimo con N, perché in quel caso possiede un inverso.

Verifica delle definizioni modulari

Controlliamo tre affermazioni usando soltanto le definizioni. La congruenza $32 \equiv 2 \pmod{15}$ è vera perché $32 - 2 = 30$ è un multiplo di 15. L'affermazione che 2 sia inverso di 8 modulo 15 è vera perché il prodotto 16 lascia resto 1.

Infine, 3 non possiede un inverso modulo 15, dato che $\gcd(3, 15) = 3$. Qualunque prodotto di 3 rimane divisibile per 3 e non può differire di 1 da un multiplo di 15. Questi controlli mostrano tre usi distinti dell'aritmetica appena costruita: riconoscere una congruenza, verificare un inverso e dimostrarne l'inesistenza. Nel capitolo seguente useremo gli stessi strumenti per studiare le potenze successive di una base.

$$32 - 2 = 2 \cdot 15$$

$$8 \cdot 2 = 15 + 1$$

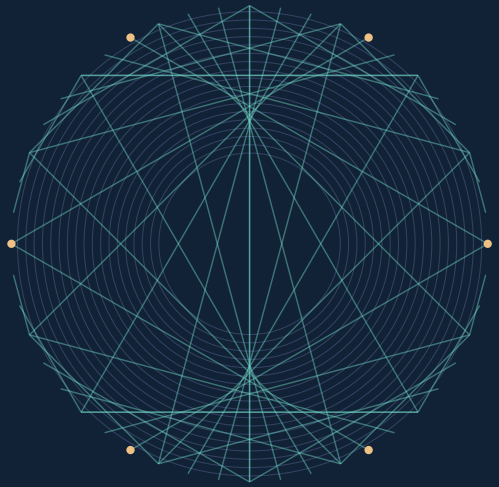
$$\gcd(3, 15) = 3$$

Richiami Congruenza: differenza multipla del modulo. Inverso: prodotto congruente a 1. Esistenza dell'inverso: MCD uguale a 1.

CAPITOLO 04

Potenze e ordine

Le ripetizioni delle potenze modulari



L’algoritmo di Shor

La base e l'esponente

Una potenza raccoglie una successione di moltiplicazioni dello stesso numero. Nella scrittura a^x, il numero a è la base e l'intero non negativo x è l'esponente. Per esempio, $2^3 = 2 \cdot 2 \cdot 2 = 8$. Aumentare di uno l'esponente significa moltiplicare ancora una volta per la base: da $2^3 = 8$ otteniamo $2^4 = 16$.

Per iniziare la successione assegniamo ad a^0 il valore 1, quando $a \neq 0$. È il valore che precede la prima moltiplicazione: $1 \cdot a = a$. Nel problema di Shor varieremo l'esponente x, mentre manterremo fissi la base a e il modulo N. La funzione che studieremo restituisce il resto della potenza, dunque un intero fra 0 e $N - 1$.

$$f(x) = a^x \bmod N, \qquad x = 0, 1, 2, \ldots$$

Richiami Il resto $v \bmod N$ è l'unico b con $0 \leq b < N$ e $v = qN + b$.

Una riduzione dopo ogni prodotto

Per trovare il resto di una potenza possiamo ridurre modulo N dopo ogni moltiplicazione. Questa scelta mantiene piccoli i numeri intermedi, perché sostituisce ciascun risultato con il suo rappresentante fra 0 e $N-1$. Le regole delle congruenze garantiscono che il resto finale rimanga lo stesso.

Consideriamo le potenze di 2 modulo 21. Dopo $2^4 = 16$, moltiplichiamo per 2 e otteniamo 32. Poiché $32 = 21 + 11$, conserviamo 11. La moltiplicazione successiva produce $2 \cdot 11 = 22$, che lascia resto 1. Abbiamo così calcolato $2^6 \bmod 21$ senza conservare la potenza intera 64. Ogni riga dipende soltanto dal resto precedente e dalla base fissata.

$$16 \cdot 2 = 32 \equiv 11 \pmod{21}$$

$$11 \cdot 2 = 22 \equiv 1 \pmod{21}$$

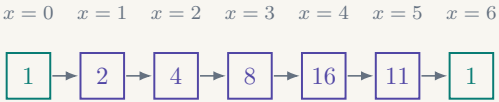
Richiami Se $u \equiv v \pmod{N}$, allora $au \equiv av \pmod{N}$: sostituire un fattore con un resto conserva la congruenza.

Le potenze di 2 modulo 21

La sequenza completa dei primi resti mette in evidenza un ritorno. All'esponente 0 abbiamo il valore 1. Seguono 2, 4, 8, 16 e 11. All'esponente 6 compare di nuovo 1. Le frecce indicano sempre la stessa operazione: moltiplicare per 2 e prendere il resto modulo 21.

La ripetizione del valore iniziale ha una conseguenza precisa. Poiché il calcolo successivo dipende soltanto dal resto corrente, dopo questo 1 otterremo ancora 2, poi 4 e tutti gli altri valori nello stesso ordine. La sequenza si ripete ogni sei passi. Per il momento abbiamo riconosciuto la ripetizione osservando tutti i valori, un procedimento utile per capire l'esempio ma costoso quando il primo ritorno è lontano.

Potenze di 2 modulo 21



Ogni passo: moltiplicare per 2 e conservare il resto

Primo ritorno a 1: $r = 6$

Ogni freccia applica una moltiplicazione per 2 modulo 21. Il secondo 1, raggiunto dopo sei passi, riporta il calcolo alla situazione iniziale.

Richiami $a^0 = 1$ e $a^{x+1} = a \cdot a^x$. Qui la base è $a = 2$ e il modulo è $N = 21$.

Il ritorno a 1 produce un periodo

La ripetizione osservata nella tabella si può giustificare per qualsiasi esponente. Sappiamo che $2^6 \equiv 1 \pmod{21}$. Moltiplicando entrambi i membri per 2^x otteniamo $2^{x+6} \equiv 2^x \pmod{21}$. Quindi due esponenti distanti sei posizioni producono sempre lo stesso resto, anche molto oltre i valori già elencati.

Chiamiamo periodo di una funzione sugli interi un intero positivo R tale che $f(x+R) = f(x)$ per tutti gli ingressi considerati. La distanza R riguarda gli esponenti, non i valori della funzione. Nel nostro esempio i valori 8 e 16 sono diversi, mentre gli ingressi 3 e 9 danno entrambi 8. La periodicità confronta proprio questi ingressi separati da sei passi.

$$2^{x+6} = 2^x 2^6 \equiv 2^x \pmod{21}$$

$$f(3) = 8 = f(9)$$

Richiami Una congruenza $u \equiv v \pmod{N}$ afferma che u e v hanno lo stesso resto nella divisione per N.

L’ordine è il primo ritorno positivo

Fra gli esponenti positivi che riportano la potenza a 1, scegliamo il più piccolo. Questo numero si chiama ordine moltiplicativo di a modulo N e lo indichiamo con r. La definizione richiede che a sia coprimo con N, condizione che tra poco giustificherà l’esistenza del ritorno.

Per $a = 2$ e $N = 21$ abbiamo $r = 6$. Gli esponenti da 1 a 5 producono 2, 4, 8, 16 e 11, mentre l’esponente 6 produce 1. L’esponente 0 non partecipa alla ricerca del minimo: tutte le basi non nulle hanno potenza zero uguale a 1, perciò quel valore non ci informa sulla lunghezza della ripetizione. Per la funzione delle potenze, l’ordine coincide con il periodo minimo.

$$r = \min\{x > 0 : \ a^x \equiv 1 \pmod{N}\}$$

$$\operatorname{ord}_{21}(2) = 6$$

Richiami Un periodo $R > 0$ soddisfa $f(x + R) = f(x)$ per ogni x. Coprimi significa $\gcd(a, N) = 1$.

Il sottogruppo percorso dalle potenze

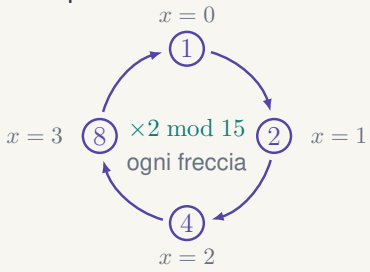
Nota facoltativa · Connessione algebrica

Riprendi il testo: p. 64

Un sottogruppo è una parte di un gruppo che contiene il neutro e rimane chiusa rispetto al prodotto e all'inversione. Le potenze di un elemento a generano un sottogruppo ciclico, indicato con $\langle a \rangle$. In un gruppo finito, se il primo ritorno a 1 avviene all'esponente r, le potenze da a^0 ad a^{r-1} sono distinte e costituiscono tutto il sottogruppo.

Per $a = 2$ modulo 15 troviamo $1, 2, 4, 8$, poi nuovamente 1. L'ordine di 2 è quindi 4 e coincide con il numero di nodi del ciclo. Il gruppo completo ha altri elementi, per esempio 7. Shor cerca la lunghezza del ciclo prodotto dalla base scelta, senza dover enumerare tutte le unità del modulo.

Le potenze di 2 modulo 15



$2^4 \equiv 1 \pmod{15}$ $\qquad r = 4$

Le frecce moltiplicano per 2 modulo 15. Gli esponenti identificano i passi. Dopo quattro moltiplicazioni si torna al neutro senza incontrare nuovi elementi.

Richiami L'ordine r di a è il minimo intero positivo con $a^r \equiv 1 \pmod{N}$. Il sottogruppo $\langle a \rangle$ contiene le potenze di a.

Un periodo può superare l'ordine

Se una successione si ripete ogni sei posizioni, si ripete anche ogni dodici o diciotto posizioni. Nel caso delle potenze la proprietà segue dal prodotto: $2^{12} = (2^6)^2$ e $2^{18} = (2^6)^3$. Entrambi lasciano resto 1 modulo 21. Tuttavia 12 e 18 non sono il primo ritorno.

Questa distinzione diventerà importante quando ricostruiremo il periodo da una misura quantistica. Il controllo $a^R \bmod N = 1$ conferma che R è un esponente di ritorno. Preso da solo, non prova che R sia minimo. Nel piccolo esempio possiamo escludere 12 come ordine perché conosciamo già il ritorno a 6. In un algoritmo occorrerà precisare quali informazioni possediamo sul candidato, invece di attribuire al controllo una conclusione più forte.

$$2^6 \equiv 2^{12} \equiv 2^{18} \equiv 1 \pmod{21}$$

Richiami L'ordine r è il minimo esponente positivo con $a^r \equiv 1 \pmod{N}$. Ogni multiplo positivo di r è un periodo.

La coprimalità garantisce il ritorno

Assumiamo $\gcd(a, N) = 1$. Esiste allora un inverso di a modulo N. Anche ogni potenza di a è invertibile: basta elevare il suo inverso allo stesso esponente. Consideriamo le $N + 1$ potenze con esponenti da 0 a N. I resti possibili sono soltanto N, quindi almeno due potenze hanno lo stesso resto. Indichiamo i loro esponenti con $i < j$.

Dalla congruenza $a^j \equiv a^i$ possiamo cancellare a^i moltiplicando per il suo inverso. Rimane $a^{j-i} \equiv 1 \pmod{N}$. L'esponente $j - i$ è positivo, dunque un ritorno esiste. Il primo di questi ritorni definisce l'ordine. La finitezza dei resti e la possibilità di cancellare spiegano insieme il risultato. Il solo fatto che i resti siano finiti non garantirebbe il ritorno proprio al valore iniziale.

$$a^j \equiv a^i \pmod{N} \quad \Longrightarrow \quad a^{j-i} \equiv 1 \pmod{N}$$

Richiami Un inverso di u modulo N è un numero v con $uv \equiv 1 \pmod{N}$. Esiste se e solo se $\gcd(u, N) = 1$.

Una successione che non ritorna a 1

La base 3 e il modulo 15 hanno un divisore comune, perciò 3 non è invertibile modulo 15. Le sue potenze producono i resti $1, 3, 9, 12, 6, 3, \ldots$. Dal secondo termine in poi compare un ciclo, ma il valore iniziale 1 non ricompare. Ogni potenza positiva è infatti divisibile per 3, mentre un numero congruente a 1 modulo 15 non lo è.

Questo esempio mostra il ruolo concreto dell'ipotesi di coprimalità. Per definire l'ordine moltiplicativo usiamo basi per cui il ritorno a 1 esiste. Nel problema della fattorizzazione, però, una base non coprima può essere già utile: $\gcd(3, 15) = 3$ fornisce immediatamente un fattore. Prima di cercare un periodo conviene dunque calcolare il massimo comun divisore.

x	$3^x \bmod 15$
0	1
1	3
2	9
3	12
4	6
5	3

La ripetizione comincia dal resto 3. L'esponente zero produce 1, che rimane esterno al ciclo delle potenze positive della base 3.

Richiami Il massimo comun divisore $\gcd(a, N)$ è il più grande intero positivo che divide sia a sia N.

L’esponente come somma di potenze di 2

Per calcolare una potenza non occorre moltiplicare la base per sé stessa tante volte quante indica l’esponente. La rappresentazione binaria permette di riutilizzare potenze già calcolate. Per esempio, $13 = 8 + 4 + 1$ e quindi $a^{13} = a^8 a^4 a$. Ogni bit uguale a 1 seleziona uno dei fattori.

Le potenze necessarie hanno esponenti $1, 2, 4, 8, \ldots$. Ciascuna si ottiene elevando al quadrato la precedente. Se lavoriamo modulo N, possiamo ridurre anche questi quadrati e i prodotti finali. La stessa organizzazione comparirà nel circuito quantistico: i bit dell’esponente decideranno quali moltiplicazioni eseguire. Qui ne studiamo prima il significato aritmetico, con un esponente classico di cui conosciamo tutti i bit.

$$13 = 1101_2 = 8 + 4 + 1$$

$$a^{13} = a^8 \, a^4 \, a^1$$

Richiami $a^{u+v} = a^u a^v$ e $(a^u)^2 = a^{2u}$. Una congruenza si conserva moltiplicando i suoi membri.

I quadrati successivi modulo 21

Applichiamo il metodo a $2^{13} \bmod 21$. Partiamo da 2, poi calcoliamo successivamente il quadrato del resto ottenuto. I resti corrispondenti agli esponenti 1, 2, 4 e 8 sono rispettivamente 2, 4, 16 e 4. L'ultimo passaggio usa $16^2 = 256 = 12 \cdot 21 + 4$.

Poiché $13 = 8 + 4 + 1$, scegliamo i resti associati agli esponenti 8, 4 e 1. Il loro prodotto vale $4 \cdot 16 \cdot 2 = 128$, che lascia resto 2 modulo 21. Volendo mantenere ancora più piccoli gli intermedi, riduciamo prima $4 \cdot 16 = 64$ al resto 1 e poi moltiplichiamo per 2. Il risultato coincide anche con la periodicità: 13 dista dodici passi dall'esponente 1.

Esponente	Potenza ridotta
1	2
2	4
4	16
8	4

Gli esponenti raddoppiano a ogni riga. Si eleva al quadrato il resto della riga precedente e si riduce il risultato modulo 21.

Richiami Per $a = 2$ modulo 21 l'ordine è 6. La scrittura $13 = 8 + 4 + 1$ seleziona tre quadrati successivi.

Calcolare una potenza e cercare l'ordine

Un esponente scritto con t bit richiede al più $t-1$ quadrati per preparare le potenze utili. I suoi bit uguali a 1 indicano poi quali moltiplicare. Il numero di prodotti cresce quindi con il numero dei bit dell'esponente, non con il suo valore numerico. Ogni prodotto modulare ha a sua volta un costo che dipende dalla lunghezza degli operandi.

La ricerca dell'ordine pone una domanda diversa. Sappiamo calcolare rapidamente il resto per un esponente assegnato, ma ignoriamo quale esponente positivo dia il primo ritorno a 1. Provare consecutivamente tutti gli esponenti fino a r può richiedere molti passi rispetto ai bit di N. Shor sfrutterà la struttura periodica della funzione mantenendo efficiente il calcolo delle singole potenze.

Dato x : $a^x \bmod N$ Da trovare: r

Richiami L'ordine è il primo $r > 0$ con $a^r \bmod N = 1$. Con t bit si rappresentano gli interi da 0 a $2^t - 1$.

Un calcolo guidato modulo 15

Calcoliamo $7^{13} \bmod 15$ con quadrati successivi. Il primo quadrato è $7^2 = 49$, che lascia resto 4. Il successivo produce $4^2 = 16$, quindi $7^4 \equiv 1$. Un altro quadrato dà $7^8 \equiv 1$. La scomposizione $13 = 8 + 4 + 1$ seleziona così i fattori 1, 1 e 7.

Il risultato è 7. Possiamo controllarlo osservando che le potenze con esponenti da 0 a 4 hanno resti $1, 7, 4, 13, 1$. Il primo ritorno positivo è 4, e 13 differisce da 1 per tre periodi completi. Il controllo tramite il periodo è comodo in questo piccolo esempio, ma il metodo dei quadrati successivi ha funzionato senza conoscere l'ordine in anticipo.

$$7^{13} = 7^8\, 7^4\, 7 \equiv 1 \cdot 1 \cdot 7 = 7 \pmod{15}$$

Richiami $a^{u+v} = a^u a^v$. L'ordine è il primo esponente positivo di ritorno a 1, non un qualsiasi esponente con resto 1.

Contare i residui coprimi

Fra i residui da 0 a 14, alcuni hanno divisori comuni con 15. Escludiamo i multipli di 3 e di 5, compreso lo zero. Rimangono $1, 2, 4, 7, 8, 11, 13, 14$. Ciascuno è coprimo con 15 e ammette quindi un inverso modulo 15. In totale abbiamo otto residui invertibili.

La funzione di Eulero, indicata con φ, conta questi residui. Scrivere $\varphi(15) = 8$ significa dunque contare gli interi fra 0 e 14 che hanno massimo comun divisore 1 con 15. La funzione dipende soltanto dal modulo. L'ordine, invece, dipende anche dalla base scelta: le potenze di 2 e quelle di 4 modulo 15 ritornano a 1 dopo un numero diverso di passi.

$$\varphi(15) = 8$$

$$\{1, 2, 4, 7, 8, 11, 13, 14\}$$

Richiami Un residuo è invertibile modulo N esattamente quando è coprimo con N, cioè quando il suo MCD con N vale 1.

Dodici residui invertibili modulo 21

Il modulo 21 ha fattori primi 3 e 7. Fra i numeri da 0 a 20, i multipli di 3 sono sette e quelli di 7 sono tre. Lo zero compare in entrambi gli elenchi. Se sottraiamo entrambi i conteggi da 21 lo escludiamo due volte, perciò dobbiamo aggiungerlo una volta nel calcolo.

Otteniamo $21 - 7 - 3 + 1 = 12$ residui coprimi. Sono $1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20$. La base 2 ne attraversa soltanto sei prima del ritorno a 1. Il numero di elementi disponibili e la lunghezza del ciclo della base sono dunque quantità diverse. Questa distinzione prepara il rapporto fra $\varphi(N)$ e l'ordine, senza identificarli.

$$\varphi(21) = 21 - 7 - 3 + 1 = 12$$

$$\operatorname{ord}_{21}(2) = 6$$

Richiami $\varphi(N)$ conta i residui coprimi con N. L'ordine r misura il primo ritorno a 1 delle potenze di una base fissata.

Il conteggio per un prodotto di due primi

Sia $N = pq$, dove p e q sono primi distinti. Fra i pq residui da 0 a $pq - 1$, i multipli di p sono q e i multipli di q sono p. L'unico residuo multiplo di entrambi è zero, perché un multiplo comune deve essere divisibile per il prodotto pq.

Escludendo questi numeri e correggendo il doppio conteggio dello zero otteniamo $pq - q - p + 1 = (p - 1)(q - 1)$. La formula riassume quindi una semplice enumerazione dei residui ammessi. Per $N = 55 = 5 \cdot 11$ dà $55 - 11 - 5 + 1 = 40$. Chi conosce i due fattori primi può calcolare subito questo valore. È precisamente l'informazione aritmetica che useremo nella preparazione delle chiavi RSA.

$$\varphi(pq) = pq - p - q + 1 = (p - 1)(q - 1)$$

$$\varphi(55) = (5 - 1)(11 - 1) = 40$$

Richiami Un numero primo ha come divisori positivi soltanto 1 e sé stesso. $\varphi(N)$ conta i residui con MCD uguale a 1.

Il teorema di Eulero

Il teorema di Eulero afferma che, se a è coprimo con N, la potenza con esponente $\varphi(N)$ lascia resto 1 modulo N. L'enunciato offre quindi un esponente di ritorno determinato dal modulo, valido per tutte le basi invertibili. Non sostiene che quel ritorno sia il primo.

Per $N = 21$, il conteggio dei residui invertibili ha dato $\varphi(21) = 12$. Il teorema garantisce $2^{12} \equiv 1$, e infatti $4096 = 195 \cdot 21 + 1$. La tabella delle potenze aveva già mostrato un ritorno all'esponente 6. Nelle pagine successive giustificheremo il teorema attraverso una permutazione dei residui e chiariremo perché l'ordine deve dividere l'esponente di Eulero.

$$\gcd(a, N) = 1 \quad \Longrightarrow \quad a^{\varphi(N)} \equiv 1 \pmod{N}$$

Richiami $\varphi(N)$ è il numero dei residui coprimi con N. L'ipotesi $\gcd(a, N) = 1$ garantisce che a sia invertibile.

Una permutazione rende visibile il teorema

Usiamo prima il modulo 10, i cui residui invertibili sono $1, 3, 7, 9$. Moltiplicandoli per 3 e riducendo modulo 10 otteniamo $3, 9, 1, 7$. Ritroviamo gli stessi quattro numeri in un altro ordine. Il loro prodotto rimane quindi congruente al prodotto iniziale.

Prima di ridurre, però, ciascuno dei quattro fattori ha ricevuto un fattore 3. Se chiamiamo P il prodotto $1 \cdot 3 \cdot 7 \cdot 9$, l'uguaglianza dei prodotti modulo 10 si scrive $3^4 P \equiv P$. Il numero P è invertibile, perché tutti i suoi fattori lo sono. Possiamo quindi cancellarlo e ottenere $3^4 \equiv 1 \pmod{10}$. L'esponente 4 è proprio il numero dei residui invertibili.

Residuo u	$3u \bmod 10$
1	3
3	9
7	1
9	7

La colonna di destra contiene esattamente gli stessi residui della prima. L'ordine cambia, mentre il prodotto modulo 10 rimane invariato.

Richiami Moltiplicare per un residuo invertibile permuta i residui invertibili. Un fattore invertibile si cancella usando il suo inverso.

La dimostrazione per un modulo qualunque

Indichiamo con $u_1, \ldots, u_m$ tutti i residui invertibili modulo N, dove $m = \varphi(N)$. Se anche a è invertibile, i prodotti $au_1, \ldots, au_m$, ridotti modulo N, sono ancora tutti invertibili e sono distinti: una coincidenza permetterebbe di cancellare a e renderebbe uguali due residui iniziali.

Abbiamo quindi una permutazione dello stesso elenco. Moltiplicando tutti gli elementi, il prodotto finale coincide modulo N con quello iniziale. Il prodotto $P = u_1 \cdots u_m$ è invertibile, perché il prodotto degli inversi dei suoi fattori ne fornisce un inverso. Cancellandolo dalla congruenza $a^m P \equiv P$, ricaviamo $a^m \equiv 1$. Poiché $m = \varphi(N)$, otteniamo l'enunciato di Eulero.

$$(au_1) \cdots (au_m) \equiv u_1 \cdots u_m \pmod{N}$$

$$a^m P \equiv P \pmod{N} \quad \Longrightarrow \quad a^m \equiv 1 \pmod{N}$$

Richiami $\varphi(N)$ conta gli invertibili. Se $uv \equiv 1 \pmod{N}$, moltiplicare una congruenza per v permette di cancellare u.

L'ordine divide ogni esponente di ritorno

Supponiamo che $a^R \equiv 1 \pmod{N}$ e che l'ordine sia r. Dividiamo l'esponente R per r: otteniamo $R = qr + s$, con $0 \leq s < r$. La potenza si separa in $(a^r)^q a^s$. Poiché $a^r \equiv 1$, il suo resto coincide con quello di a^s.

Ma avevamo assunto che il resto di a^R fosse 1. Dunque anche $a^s \equiv 1$. Se s fosse positivo, avremmo un ritorno precedente a r, in contrasto con la definizione dell'ordine. Deve quindi essere $s = 0$, cioè r divide R. Applicando il ragionamento all'esponente $R = \varphi(N)$ fornito da Eulero, concludiamo che l'ordine divide sempre $\varphi(N)$.

$$a^R = (a^r)^q a^s \equiv a^s \pmod{N}$$

$$r \mid \varphi(N)$$

Richiami L'ordine r è il minimo esponente positivo di ritorno. La divisione con resto scrive $R = qr + s$ con $0 \leq s < r$.

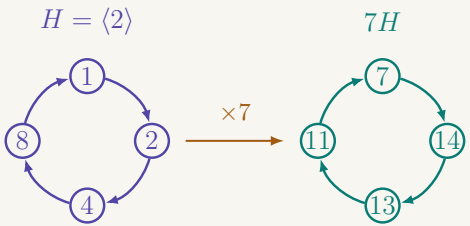
Le classi laterali di un sottogruppo

Nota facoltativa · Connessione algebrica

Riprendi il testo: p. 80

Sia H un sottogruppo di G. Per un elemento g di G, la classe laterale gH è l'insieme dei prodotti gh, con h che percorre H. Moltiplichiamo dunque tutti gli elementi di H per uno stesso elemento. La moltiplicazione è invertibile, perciò ogni classe contiene tanti elementi quanti ne contiene H.

Prendiamo $H = \langle 2 \rangle = \{1, 2, 4, 8\}$ modulo 15. Moltiplicando per 7 otteniamo $7H = \{7, 14, 13, 11\}$. Le due classi non condividono elementi e insieme comprendono tutte le otto unità. La classe $7H$ non è un sottogruppo, perché non contiene 1. Questa suddivisione prepara il conteggio che collega l'ordine della base alla dimensione del gruppo.



Nei cicli: moltiplicazione per 2 modulo 15.

La freccia fra i cicli applica il prodotto per 7. Le corrispondenze riportate sotto associano gli elementi delle due classi, sempre modulo 15.

Richiami $gH = \{gh : h \in H\}$. La moltiplicazione per g è invertibile e conserva il numero degli elementi.

Il conteggio delle classi e il teorema di Lagrange

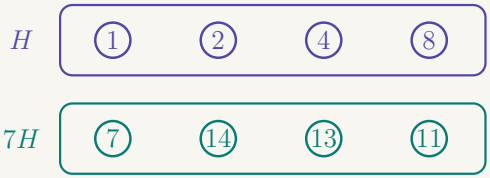
Nota facoltativa · Connessione algebrica

Riprendi il testo: p. 80

Le classi laterali di un sottogruppo finito hanno tutte la stessa dimensione. Inoltre due classi sono uguali oppure disgiunte: se condividono un elemento, l'inversione permette di ricondurre ogni elemento dell'una all'altra. Poiché ogni elemento del gruppo appartiene a una classe, queste classi suddividono il gruppo senza sovrapposizioni.

Per un gruppo finito G, indichiamo con $|G|$ il numero dei suoi elementi. Il teorema di Lagrange afferma che $|H|$ divide $|G|$. Nell'esempio ci sono due classi da quattro elementi, quindi $8 = 2 \cdot 4$. Scegliendo $G = \mathbb{Z}_N^\times$ e $H = \langle a \rangle$, otteniamo $r \mid \varphi(N)$. Il numero degli invertibili è dunque un multiplo dell'ordine, ma non lo determina: basi diverse possono generare sottogruppi di dimensioni diverse.

Gli otto elementi di $\mathbb{Z}_{15}^\times$



$$|G| = 2\,|H| = 2 \cdot 4 = 8$$

Le due classi sono disgiunte e coprono il gruppo.

$$|G| = 2|H| = 8, \qquad r = 4 \mid 8$$

Le due classi esauriscono le otto unità modulo 15. Il conteggio delle classi di uguale dimensione rende visibile la divisibilità del teorema di Lagrange.

Richiami $\varphi(N) = |\mathbb{Z}_N^\times|$ conta i residui invertibili. Il sottogruppo generato da a contiene r elementi.

Il caso di un modulo primo

Se il modulo p è primo, ogni residuo da 1 a $p-1$ è coprimo con p. L'unico residuo escluso è zero, perciò $\varphi(p) = p-1$. Il teorema di Eulero assume allora la forma $a^{p-1} \equiv 1 \pmod{p}$, purché a non sia divisibile per p. Questo risultato prende il nome di piccolo teorema di Fermat.

Per esempio, modulo 5 la base 2 soddisfa $2^4 = 16 \equiv 1$. La base 5, invece, ha resto zero e ogni sua potenza positiva resta congruente a zero. L'ipotesi sull'assenza di divisibilità è quindi essenziale. Nella dimostrazione di correttezza di RSA useremo Fermat separatamente modulo ciascuno dei due fattori primi, trattando a parte proprio il caso di resto zero.

$$p \nmid a \quad \Longrightarrow \quad a^{p-1} \equiv 1 \pmod{p}$$

Richiami Eulero: se $\gcd(a, N) = 1$, allora $a^{\varphi(N)} \equiv 1 \pmod{N}$. Per un primo p, vale $\varphi(p) = p-1$.

Base, ordine e numero di invertibili

Il modulo 15 permette di confrontare le quantità appena introdotte. Il suo numero di residui invertibili è sempre 8. La base 2 ha ordine 4, perché le prime potenze positive producono $2, 4, 8, 1$. La base 4 ha ordine 2, perché $4^2 = 16 \equiv 1$. La base 1 ha ordine 1.

Gli ordini cambiano con la base, ma dividono tutti 8. Perciò il teorema di Eulero assegna a queste basi uno stesso esponente di ritorno senza affermare che abbiano lo stesso ciclo. Nella ricerca del periodo manterremo fissata una base e cercheremo il suo ordine. Nella costruzione di RSA useremo invece un esponente che funzioni per tutti i messaggi coprimi, grazie al valore comune $\varphi(N)$.

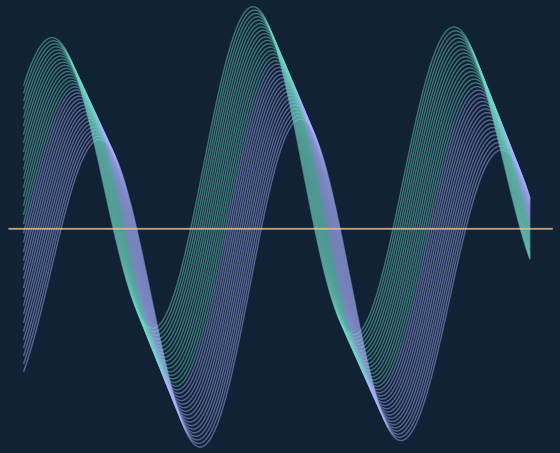
Base a	**Ordine modulo 15**	$\varphi(15)$
1	1	8
2	4	8
4	2	8

Il conteggio degli invertibili è una proprietà del modulo. L'ordine descrive invece la successione generata dalla base scelta, come mostrano le tre righe.

Richiami $\varphi(N)$ dipende dal modulo. L'ordine dipende dalla coppia (a, N) e divide $\varphi(N)$.

CAPITOLO 05

La costruzione di RSA



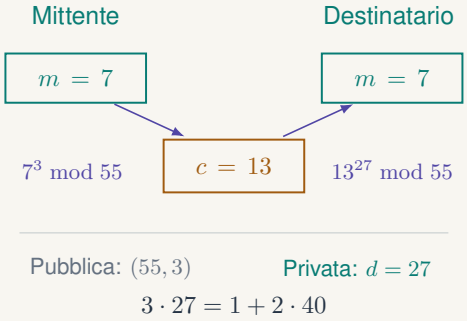
Chiavi, cifratura e correttezza della decifratura

L'algoritmo di Shor

Una chiave pubblica per ricevere messaggi

Consideriamo una comunicazione nella quale il destinatario desidera pubblicare le istruzioni per cifrare, conservando per sé l'informazione necessaria a decifrare. In RSA la chiave pubblica contiene un modulo N e un esponente e. Il mittente rappresenta il messaggio mediante un intero m compreso fra 0 e $N-1$ e calcola il resto di m^e.

Il destinatario usa un altro esponente, indicato con d, per recuperare il messaggio dal cifrato. Costruiremo questi dati con numeri piccoli, seguendo ogni passaggio aritmetico. Gli esempi servono a spiegare la relazione fra le due operazioni e non costituiscono parametri sicuri. Inoltre studieremo dapprima la trasformazione aritmetica, mentre uno schema di cifratura per applicazioni richiede ulteriori accorgimenti.



Il mittente usa i dati pubblici per produrre il cifrato. Il destinatario conserva l'esponente di decifratura. Nelle pagine successive ricaveremo tutti questi numeri.

Richiami Una potenza modulare restituisce un resto fra 0 e $N-1$. I quadrati successivi consentono di calcolarla senza costruire l'intera potenza.

La scelta dei due primi

Il destinatario comincia scegliendo due numeri primi distinti. Nel nostro esempio sono $p = 5$ e $q = 11$. Il loro prodotto è $N = 55$, che diventa il modulo pubblico. In questo modo i messaggi aritmetici sono i 55 interi da 0 a 54, e anche ogni cifrato appartiene allo stesso intervallo.

Il destinatario conosce la fattorizzazione perché ha costruito il prodotto. Chi osserva soltanto il modulo deve invece ricavarla, se vuole ottenere i fattori con quella via. Per il piccolo numero 55 bastano pochi tentativi, mentre l'interesse dell'algoritmo riguarda numeri molto più grandi. La distinzione fra conoscere i fattori e conoscere soltanto il prodotto spiega quali informazioni terremo separate nel racconto.

$$p = 5, \qquad q = 11, \qquad N = pq = 55$$

Richiami Un primo ha soltanto due divisori positivi. Per due primi distinti p, q, il prodotto $N = pq$ determina il modulo RSA.

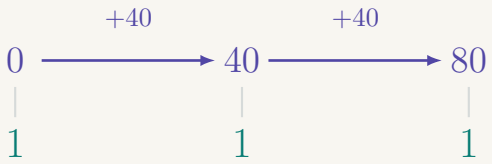
L’esponente comune alle basi coprime

Il destinatario conosce i due primi 5 e 11 e può quindi calcolare $\varphi(55) = (5-1)(11-1) = 40$. Il simbolo $\varphi(55)$ conta i resti coprimi con 55, cioè quelli il cui massimo comun divisore con 55 vale 1.

Per ciascuno di questi resti m, il teorema di Eulero garantisce $m^{40} \equiv 1 \pmod{55}$. Quaranta è dunque un esponente di ritorno valido per tutte le basi coprime. Il primo ritorno di una particolare base può avvenire prima.

Moltiplicando per m otteniamo $m^{41} \equiv m$. Ripetendo il ragionamento, anche m^{81} ha lo stesso resto di m. La costruzione di RSA sceglierà due esponenti il cui prodotto realizzi proprio uno di questi ritorni al messaggio iniziale.

Se $\gcd(m, 55) = 1$: potenze di m



In alto: esponente

In basso: resto della potenza

Ritorni garantiti da Eulero. Il primo ritorno può avvenire prima di 40.

Richiami $\gcd(m, N) = 1$: m e N sono coprimi. Eulero: $m^{\varphi(N)} \equiv 1 \pmod{N}$. Per $N = pq$, $\varphi(N) = (p-1)(q-1)$.

Gli esponenti che restituiscono il messaggio

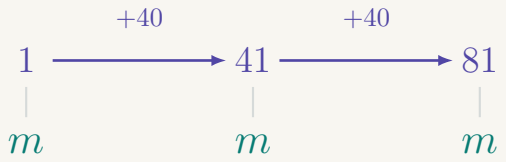
Partiamo ora dall'esponente 1, che rappresenta il messaggio m stesso. Aggiungere 40 all'esponente equivale a moltiplicare la potenza per m^{40}. Se m è coprimo con 55, quel fattore vale 1 modulo 55 e il resto non cambia.

Gli esponenti 1, 41 e 81 restituiscono quindi tutti m. Più in generale, lo stesso accade per $1 + 40k$, con k intero non negativo:

$$m^{1+40k} = m(m^{40})^k \equiv m \pmod{55}.$$

La decifratura dovrà produrre una potenza con questa forma. Il suo esponente dipenderà dalla composizione di due elevamenti a potenza: per questo cerchiamo una condizione sul prodotto ed.

Potenze con lo stesso resto del messaggio



In alto: esponente

In basso: resto della potenza

Per recuperare il messaggio è sufficiente raggiungere uno degli esponenti $1 + 40k$.

Richiami Aggiungere 40 all'esponente moltiplica la potenza per $m^{40} \equiv 1$. La condizione richiede $\gcd(m, 55) = 1$.

La scelta dell'esponente pubblico

Scegliamo $e = 3$ e cerchiamo un intero positivo d per il quale $3d$ abbia la forma $1 + 40k$. In termini di congruenze, chiediamo $3d \equiv 1 \pmod{40}$. Il numero d sarà un inverso moltiplicativo di 3 modulo 40.

Un inverso esiste quando il numero da invertire è coprimo con il modulo. Qui $\gcd(3, 40) = 1$, quindi la scelta è ammessa. Il controllo riguarda $40 = \varphi(55)$, perché è il ritorno comune che stiamo usando per gli esponenti.

La scelta $e = 2$ non funzionerebbe: ogni prodotto $2d$ è pari, mentre $1 + 40k$ è sempre dispari. Il fatto che 2 sia coprimo con 55 non risolve questa incompatibilità. Occorre controllare $\gcd(e, \varphi(N)) = 1$.

$$e = 3$$

$$3d = 1 + 40k$$

$$\gcd(3, 40) = 1$$

L'inverso esiste.

$e = 2$: pari $\neq$ dispari

La coprimalità necessaria riguarda l'esponente e il modulo usato per costruirne l'inverso.

Richiami d è un inverso di e modulo M se $ed \equiv 1 \pmod{M}$. Un inverso esiste esattamente quando $\gcd(e, M) = 1$.

Il calcolo dell'esponente privato

La divisione $40 = 13 \cdot 3 + 1$ esprime il resto 1 come combinazione di 40 e 3. Portando il prodotto dall'altra parte otteniamo $1 = 40 - 13 \cdot 3$.

Modulo 40, il termine 40 scompare e rimane $(-13) \cdot 3 \equiv 1$. Un inverso di 3 è dunque -13. Aggiungendo 40 scegliamo il rappresentante positivo $d = 27$, che ha la stessa proprietà.

Il controllo fornisce $3 \cdot 27 = 81 = 1 + 2 \cdot 40$. L'esponente d realizza quindi il prodotto richiesto. L'inversione riguarda numeri interi e resti: 27 non rappresenta il reciproco ordinario $1/3$, ma un numero che moltiplicato per 3 lascia resto 1 modulo 40.

$$40 = 13 \cdot 3 + 1$$

$$1 = 40 - 13 \cdot 3$$

$$\downarrow$$

$$d \equiv -13 \equiv 27 \pmod{40}$$

$$3 \cdot 27 = \underbrace{80}_{2 \cdot 40} + 1$$

La divisione con resto consente di ricostruire l'inverso moltiplicativo.

Richiami $-13 \equiv 27 \pmod{40}$, perché $27 - (-13) = 40$. La chiave usa $e = 3$, $d = 27$ e $ed = 81$.

Il ruolo dell'esponente privato

Una volta costruita la chiave, $d = 27$ rimane fisso. Il destinatario lo usa per ogni cifrato ricevuto con questa chiave, indipendentemente dal valore del messaggio.

Cifrare significa elevare m alla terza potenza modulo 55. Decifrare significa elevare quel risultato alla ventisettesima potenza, sempre modulo 55. La composizione produce dunque $(m^3)^{27} = m^{81}$.

La moltiplicazione $3 \cdot 27$ riguarda gli esponenti. Non aggiungiamo 27 all'esponente 3 e non percorriamo necessariamente 27 passi del ciclo delle potenze di m. Il legame utile con la periodicità è $81 = 1 + 2 \cdot 40$: per una base coprima, questa potenza restituisce lo stesso resto di m^1.

Composizione delle due operazioni

$$m$$

$$\downarrow \quad \text{potenza } e = 3$$

$$m^3 \bmod 55$$

$$\downarrow \quad \text{potenza } d = 27$$

$$m^{81} \bmod 55$$

Esponente complessivo: $3 \cdot 27 = 81$

d moltiplica l'esponente pubblico. Il prodotto è 81, non 30.

Richiami $(m^e)^d = m^{ed}$. d è un esponente di decifratura fissato dalla chiave. L'ordine di una base è invece il suo primo esponente di ritorno a 1.

Il modulo dei messaggi e quello degli esponenti

La chiave pubblica è $(N, e) = (55, 3)$ e l'esponente privato è $d = 27$. Tutte le potenze che trasformano un messaggio o un cifrato vengono ridotte modulo 55.

Il numero 40 compare invece nella relazione fra gli esponenti: $3 \cdot 27 \equiv 1 \pmod{40}$. Lo abbiamo calcolato dai fattori di 55 e usato per costruire un prodotto che restituisca il messaggio.

Le due congruenze hanno quindi oggetti diversi. In $c = m^3 \bmod 55$ riduciamo una potenza del messaggio. In $3d \equiv 1 \pmod{40}$ riduciamo un prodotto di esponenti. Il teorema di Eulero collega le due operazioni, perché garantisce che aggiungere 40 all'esponente di una base coprima non ne cambia il resto modulo 55.

Operazioni sui messaggi

$$c = m^3 \bmod 55$$

$$m = c^{27} \bmod 55$$

Relazione fra gli esponenti

$$3 \cdot 27 \equiv 1 \pmod{40}$$

I due moduli rimangono distinti in ogni passaggio del calcolo.

Richiami Messaggi: $c = m^e \bmod N$, $m = c^d \bmod N$. Costruzione della chiave: $ed \equiv 1 \pmod{\varphi(N)}$.

La cifratura del messaggio 7

Il mittente vuole inviare il messaggio aritmetico $m = 7$. Conosce soltanto i dati pubblici necessari, cioè $N = 55$ ed $e = 3$. Calcola $7^3 = 343$ e divide per 55. Poiché $343 = 6 \cdot 55 + 13$, il cifrato è $c = 13$.

Il simbolo c indica qui il resto trasmesso al destinatario. Per eseguire questo calcolo non servono né i fattori 5 e 11 né l'esponente privato 27. Questa asimmetria delle informazioni è lo scopo della costruzione. Nei numeri del nostro esempio la cifratura si può svolgere mentalmente, ma la stessa operazione, mediante quadrati successivi, si applica anche quando l'esponente e il modulo richiedono molti bit.

$$c = 7^3 \bmod 55 = 343 \bmod 55 = 13$$

Richiami La chiave pubblica è $(N, e) = (55, 3)$. Il messaggio aritmetico soddisfa $0 \leq m < N$ e il cifrato è $c = m^e \bmod N$.

Le potenze necessarie per decifrare

Il destinatario riceve $c = 13$ e deve calcolare $13^{27} \bmod 55$. La rappresentazione binaria dell'esponente è $27 = 16 + 8 + 2 + 1$. Prepariamo quindi i resti delle potenze con esponenti 1, 2, 4, 8 e 16, elevando ogni volta al quadrato il resto precedente.

I primi due passaggi danno $13^2 = 169 \equiv 4$ e $13^4 \equiv 4^2 = 16$. Seguono $16^2 = 256 \equiv 36$ e $36^2 = 1296 \equiv 31$. Per la ricomposizione useremo le righe degli esponenti 16, 8, 2 e 1. La riga dell'esponente 4 è servita a costruire le successive, ma il relativo bit di 27 è zero, quindi non entra nel prodotto finale.

Esponente	$13^{\text{esponente}} \bmod 55$
1	13
2	4
4	16
8	36
16	31

Ogni resto si ottiene dal quadrato del precedente. L'esponente 27 seleziona le righe 16, 8, 2 e 1 per la moltiplicazione conclusiva.

Richiami Quadrati successivi: $(a^{2^j})^2 = a^{2^{j+1}}$. La riduzione modulo N si può effettuare dopo ogni prodotto.

Il recupero del messaggio

Combiniamo i resti selezionati dalla scomposizione di 27. Il prodotto corrispondente è $31 \cdot 36 \cdot 4 \cdot 13$. Riduciamo dopo ciascuna moltiplicazione: $31 \cdot 36 = 1116$ lascia resto 16 modulo 55. Poi $16 \cdot 4 = 64$ lascia resto 9. Infine $9 \cdot 13 = 117$ lascia resto 7.

Abbiamo recuperato il messaggio iniziale. La sequenza completa è dunque una cifratura che associa 7 a 13 e una decifratura che riporta 13 a 7. Tutti i passaggi hanno usato soltanto moltiplicazioni e divisioni con resto. Rimane da spiegare perché la relazione fra gli esponenti garantisca questo risultato, invece di limitarci alla verifica di una coppia particolare.

$$31 \cdot 36 \equiv 16, \quad 16 \cdot 4 \equiv 9, \quad 9 \cdot 13 \equiv 7 \pmod{55}$$

$$13^{27} \bmod 55 = 7$$

Richiami $27 = 16 + 8 + 2 + 1$. I resti di $13^{16}, 13^{8}, 13^{2}, 13$ modulo 55 sono rispettivamente $31, 36, 4, 13$.

La composizione delle potenze

Il calcolo numerico ha restituito 7. Per spiegare il risultato, riscriviamo la cifratura e la decifratura come un'unica potenza del messaggio.

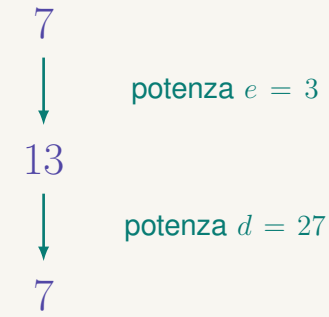
Poiché $c \equiv m^3 \pmod{55}$, anche le ventisettesime potenze sono congruenti: $c^{27} \equiv (m^3)^{27} = m^{81}$. Ridurre il cifrato prima del secondo elevamento non cambia il resto conclusivo.

Per il messaggio 7, che è coprimo con 55, Eulero dà $7^{40} \equiv 1$. Pertanto

$$7^{81} = 7(7^{40})^2 \equiv 7.$$

Il ritorno al messaggio dipende così dalla scelta degli esponenti. La verifica numerica delle potenze e questa giustificazione descrivono lo stesso procedimento da due punti di vista complementari.

Composizione delle due operazioni



Esponente complessivo: $3 \cdot 27 = 81$

Ogni freccia rappresenta un elevamento a potenza modulo 55.

Richiami Le congruenze si conservano elevando entrambi i membri alla stessa potenza intera non negativa. Qui $ed = 81 = 1 + 2 \cdot 40$.

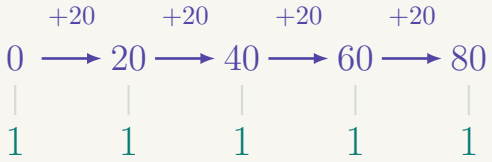
Il primo ritorno di 7 e l'esponente comune 40

Per la base 7, il primo ritorno a 1 modulo 55 avviene all'esponente 20. Possiamo verificarlo senza elencare tutte le potenze: $7^{20} \equiv 1$, mentre $7^{10} \equiv 34 \neq 1$ e $7^4 \equiv 36 \neq 1$. I divisori propri di 20 sono $1, 2, 4, 5, 10$: ciascuno divide 4 oppure 10. Gli ultimi due controlli li escludono quindi tutti come ordini possibili.

Il ritorno garantito da Eulero all'esponente 40 comprende quindi due periodi minimi. Questo basta per RSA: $81 - 1 = 80$ contiene quattro periodi di lunghezza 20, oppure due blocchi di lunghezza 40.

Il valore $d = 27$ resta un'altra quantità ancora: moltiplica l'esponente pubblico 3 e produce 81. Per costruire la chiave usiamo un esponente comune, senza dover conoscere l'ordine di ogni possibile messaggio.

Ritorni a 1 delle potenze di 7



In alto: esponente

In basso: resto della potenza

Sono rappresentati soltanto i ritorni: 40 comprende due periodi di lunghezza 20.

Richiami L'ordine è il minimo $r > 0$ con $a^r \equiv 1 \pmod{N}$. Se $a^t \equiv 1$, allora $r \mid t$. Qui $\mathrm{ord}_{55}(7) = 20$ e $\varphi(55) = 40$.

La correttezza per i messaggi coprimi

Il ragionamento non dipende dal valore particolare 7. Supponiamo che $N = pq$ con primi distinti e che gli esponenti soddisfino $ed = 1 + k\varphi(N)$. Per ogni messaggio m coprimo con N, il teorema di Eulero fornisce $m^{\varphi(N)} \equiv 1$.

La composizione della cifratura e della decifratura restituisce quindi

$$m^{ed} = m\Big(m^{\varphi(N)}\Big)^{k} \equiv m \pmod{N}.$$

Il messaggio iniziale e il risultato finale, ridotto modulo N, appartengono entrambi all'intervallo da 0 a $N-1$. Due numeri in questo intervallo con lo stesso resto modulo N coincidono: la loro differenza non può essere un multiplo non nullo di N.

Abbiamo dunque recuperato esattamente il messaggio. Resta da esaminare il caso in cui il messaggio abbia un fattore comune con N, perché in quel caso manca l'ipotesi necessaria per applicare Eulero.

Richiami RSA richiede $ed \equiv 1 \pmod{\varphi(N)}$. L'argomento di questa pagina usa inoltre $\gcd(m, N) = 1$.

La cifratura come automorfismo degli invertibili

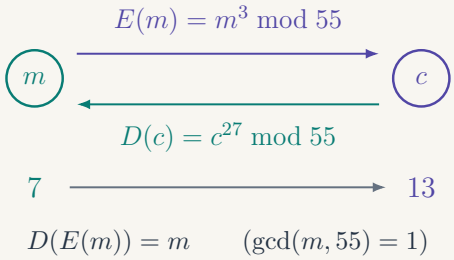
Nota facoltativa · Connessione algebrica

Riprendi il testo: p. 98

Un automorfismo di un gruppo è una corrispondenza biunivoca del gruppo con sé stesso che conserva l'operazione. Biunivoca significa che ogni uscita proviene da un solo ingresso. Sul gruppo commutativo $\mathbb{Z}_{55}^{\times}$, la funzione $E(m) = m^3 \bmod 55$ conserva i prodotti, perché $(uv)^3 = u^3 v^3$.

Il teorema di Eulero dà $m^{40} \equiv 1$ per ogni elemento del gruppo. Poiché $3 \cdot 27 = 81 = 1 + 2 \cdot 40$, la funzione $D(c) = c^{27} \bmod 55$ inverte E, rendendola biunivoca. Il percorso $7, 13, 7$ è un esempio. Questa lettura riguarda gli invertibili. La correttezza per i messaggi non coprimi richiede l'argomento successivo sui due primi. Nel capitolo 6 il periodo delle potenze del cifrato permetterà di costruire un esponente sufficiente a recuperare il messaggio.

Una permutazione degli invertibili modulo 55



Il diagramma mostra due trasformazioni inverse sul gruppo degli invertibili. La corrispondenza fra 7 e 13 illustra il percorso di un singolo messaggio.

Richiami RSA nell'esempio: $N = 55$, $e = 3$, $d = 27$, $ed \equiv 1 \pmod{40}$. Eulero richiede $\gcd(m, 55) = 1$.

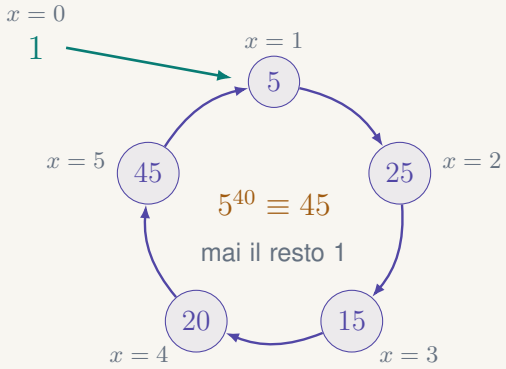
Il messaggio 5 e l'ipotesi di coprimalità

Il messaggio $m = 5$ è ammesso, perché appartiene all'intervallo da 0 a 54. Tuttavia $\gcd(5, 55) = 5$, quindi il teorema di Eulero non assicura $5^{40} \equiv 1 \pmod{55}$. Il calcolo dà infatti resto 45.

Il diagramma mostra la successione delle potenze: dopo il termine iniziale $5^0 = 1$, i valori positivi percorrono il ciclo $5, 25, 15, 20, 45$ e ricominciano da 5. Il resto 1 non riappare.

RSA recupera ugualmente il messaggio: $5^3 \bmod 55 = 15$ e $15^{27} \bmod 55 = 5$. La chiave rimane $d = 27$. Per giustificare il risultato serve però un argomento che tenga conto dei due fattori del modulo e tratti separatamente il resto zero.

Potenze positive di 5 modulo 55



Ogni freccia: $\times 5 \pmod{55}$

Gli esponenti 40 e 81 raggiungono rispettivamente i valori 45 e 5.

Richiami Eulero richiede $\gcd(m, N) = 1$. Una successione di potenze di una base non coprima può avere un ciclo senza ritornare a 1.

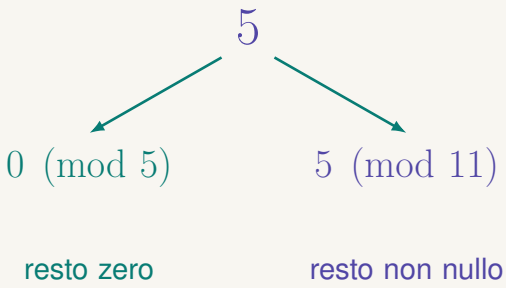
Il messaggio osservato nei due moduli primi

Il numero 55 è il prodotto di 5 e 11. Per seguire una potenza modulo 55, possiamo prima studiarne i resti rispetto a questi due moduli più piccoli e poi ricomporre l'informazione.

Il messaggio 5 lascia resto 0 modulo 5 e resto 5 modulo 11. Nel primo caso ogni potenza positiva resta divisibile per 5. Nel secondo caso la base è coprima con 11, perché un primo non divide nessuno dei resti non nulli più piccoli di sé.

Useremo perciò due argomenti diversi, ciascuno adatto al resto osservato. Alla fine mostreremo che conoscere entrambi i resti determina un unico risultato modulo 55. Non stiamo cambiando messaggio o chiave, ma osservando lo stesso calcolo attraverso i due fattori del modulo.

Lo stesso messaggio $m = 5$



Il modulo determina quale argomento usare.

Resto zero: divisibilità. Resto non nullo: teorema di Eulero.

Richiami $5 \equiv 0 \pmod 5$ e $5 \equiv 5 \pmod{11}$. Per un primo p, ogni resto non nullo modulo p è coprimo con p.

Il teorema di Eulero per un modulo primo

Se il modulo è un primo p, i resti $1, 2, \ldots, p-1$ sono tutti coprimi con esso. Sono $p-1$, quindi $\varphi(p) = p-1$. Applicando Eulero a una base non divisibile per p, otteniamo

$$m^{p-1} \equiv 1 \pmod{p}.$$

Questa forma del risultato prende il nome di piccolo teorema di Fermat. È dunque lo stesso principio di ritorno già usato, specializzato a un modulo primo.

Per $p = 11$, l'esponente garantito è 10. Poiché 5 non è divisibile per 11, abbiamo $5^{10} \equiv 1 \pmod{11}$. Il teorema non si applica al resto zero nella forma appena scritta: ogni sua potenza positiva ha ancora resto zero.

Modulo primo $p = 11$

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10$$

dieci resti coprimi

$$\varphi(11) = 10$$

$$5^{10} \equiv 1 \pmod{11}$$

Fermat è la forma di Eulero per un modulo primo.

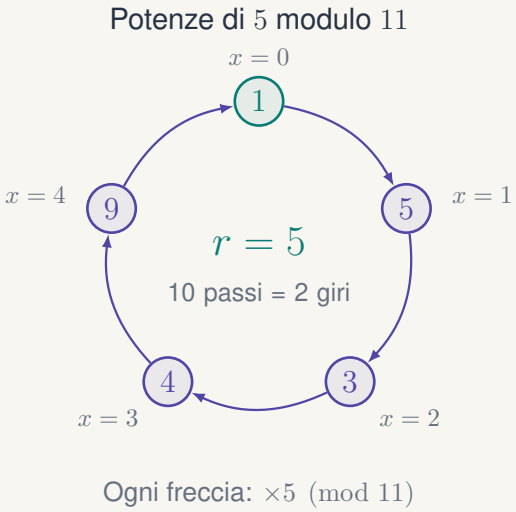
Richiami Per un primo p, $\varphi(p) = p-1$. Se $p \nmid m$, Fermat dà $m^{p-1} \equiv 1 \pmod{p}$.

Il ciclo delle potenze di 5 modulo 11

Le potenze di 5 modulo 11 hanno resti $1, 5, 3, 4, 9, 1$. Ogni freccia del diagramma moltiplica il resto corrente per 5 e conserva il resto della divisione per 11.

Il primo ritorno a 1 avviene dopo cinque passi, quindi l'ordine di 5 modulo 11 è 5. Il teorema di Fermat garantisce il ritorno all'esponente 10, che in questo caso comprende due giri completi.

La distinzione fra primo ritorno e ritorno garantito rimane la stessa incontrata con Eulero. Per dimostrare la correttezza della chiave basta il ritorno comune di lunghezza 10, disponibile per ogni messaggio non nullo modulo 11. Non occorre determinare prima il periodo particolare di ciascun messaggio.



Cinque passi formano un giro. Fermat garantisce il ritorno dopo dieci passi.

Richiami $\mathrm{ord}_{11}(5) = 5$, mentre $\varphi(11) = 10$. Un multiplo del periodo minimo produce anch'esso un ritorno a 1.

L’esponente 81 restituisce il resto 5 modulo 11

La cifratura seguita dalla decifratura produce $5^{ed} = 5^{81}$. Per studiarla modulo 11, scriviamo $81 = 1 + 8 \cdot 10$.

Il fattore corrispondente ai primi 80 passi è una potenza di 5^{10}, che vale 1 modulo 11. Rimane quindi un solo fattore 5:

$$5^{81} = 5(5^{10})^8 \equiv 5 \pmod{11}.$$

Nel ciclo della pagina precedente, gli 80 passi formano sedici giri completi. Il passo rimanente raggiunge nuovamente il nodo 5.

La scelta di d rende possibile questa scomposizione perché $ed - 1 = 80$ è multiplo di 40, e quindi anche di $10 = 11 - 1$ e di $4 = 5 - 1$. La stessa chiave rispetta così i ritorni garantiti nei due moduli primi.

$$ed - 1 = 81 - 1 = 80$$

$80 = 2 \cdot 40$



$80 = 20 \cdot 4$



$80 = 8 \cdot 10$



$40 = \varphi(55), \qquad 4 = 5 - 1, \qquad 10 = 11 - 1$

Lo stesso numero 80, suddiviso secondo i tre esponenti di ritorno garantiti.

Richiami $e = 3$, $d = 27$, $ed - 1 = 80 = 2 \cdot 40 = 20 \cdot 4 = 8 \cdot 10$. Modulo 11, $5^{10} \equiv 1$.

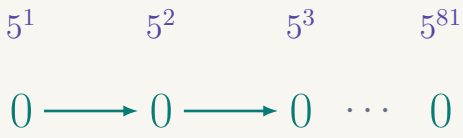
Il resto zero modulo 5

Osserviamo ora lo stesso messaggio modulo 5. Ogni potenza positiva 5^k contiene il fattore 5, quindi lascia resto zero. In particolare, $5^{81} \equiv 0 \pmod 5$.

Anche il messaggio iniziale 5 ha resto zero. Otteniamo dunque $5^{81} \equiv 5 \pmod 5$ senza applicare alcun teorema sugli inversi.

Questo ramo del ragionamento è necessario per tutti i messaggi divisibili per uno dei fattori del modulo. La potenza m^{p-1} non vale 1 quando p divide m: vale 0. La correttezza segue comunque, perché il messaggio e il risultato della composizione hanno entrambi quel resto.

Potenze positive modulo 5



$5^k = 5 \cdot 5^{k-1}$, per $k \geq 1$

Ogni termine contiene il fattore 5.

Sono rappresentati esponenti positivi. L'esponente zero, escluso dalla figura, dà 1.

Richiami Se $p \mid m$, allora $p \mid m^k$ per ogni intero $k \geq 1$. Qui $ed = 81$ è positivo e $5 \mid m$.

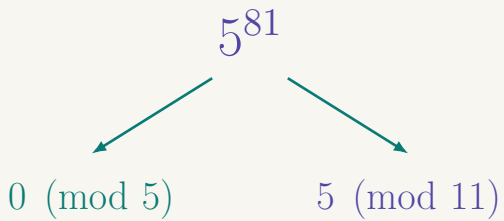
I due resti della potenza finale

Abbiamo studiato 5^{81} attraverso due moduli, mantenendo sempre lo stesso messaggio e gli stessi esponenti. Il calcolo modulo 5 dà resto 0. Il calcolo modulo 11 dà resto 5.

Sono esattamente i due resti del messaggio iniziale. Il risultato finale della decifratura, ridotto all'intervallo da 0 a 54, deve quindi soddisfare entrambe le condizioni:

$$u \equiv 0 \pmod 5, \qquad u \equiv 5 \pmod{11}.$$

Rimane da capire perché queste condizioni individuino un solo numero. La prima restringe la scelta ai multipli di 5. La seconda seleziona, fra questi, quello con resto 5 modulo 11. Nel nostro esempio possiamo vedere questa selezione direttamente.



Sono anche i resti del messaggio 5.

$$u \in \{0, 1, \ldots, 54\}$$

Ciascuna condizione lascia più candidati. Insieme individuano il risultato.

Richiami Il risultato della decifratura è $u = 15^{27} \bmod 55 = 5^{81} \bmod 55$. Per costruzione, $0 \leq u < 55$.

L’unico candidato fra 0 e 54

I numeri fra 0 e 54 con resto zero modulo 5 sono $0, 5, 10, \ldots, 50$. La tabella riporta, accanto a ciascuno, il resto modulo 11.

Fra questi undici candidati, soltanto 5 lascia resto 5 modulo 11. La decifratura deve quindi restituire proprio 5. Abbiamo giustificato il risultato senza calcolare per esteso l’enorme intero 5^{81}.

La tabella rende visibile il meccanismo: il primo resto seleziona una famiglia di numeri e il secondo elimina l’ambiguità. Per moduli più grandi non costruiremo questa lista. Useremo invece la coprimalità dei due fattori per dimostrare che due candidati con entrambi i resti uguali devono coincidere modulo il loro prodotto.

Candidati con resto zero modulo 5

u	$u \bmod 11$	
0	0	
5	5	scelto
10	10	
15	4	
20	9	
25	3	
30	8	
35	2	
40	7	
45	1	
50	6	

Ogni riga soddisfa il primo vincolo. La riga evidenziata soddisfa anche il secondo.

Richiami $u \equiv 0 \pmod 5$ significa $u = 5k$. Il secondo vincolo è $u \equiv 5 \pmod{11}$. Inoltre $0 \le u < 55$.

La ricomposizione mediante i due fattori

Supponiamo che due interi u e v abbiano lo stesso resto modulo 5 e lo stesso resto modulo 11. Allora la differenza $u - v$ è divisibile per entrambi. Poiché 5 e 11 sono primi distinti, la differenza contiene entrambi i fattori e quindi è divisibile per 55.

Ne segue $u \equiv v \pmod{55}$. Se entrambi sono compresi fra 0 e 54, devono essere uguali. Lo stesso argomento vale per $N = pq$, con p e q primi distinti.

Nel nostro caso $u = 5^{81}$ e $v = 5$ hanno gli stessi resti nei due moduli primi. Perciò $5^{81} \equiv 5 \pmod{55}$, e la riduzione finale restituisce il messaggio 5. La coprimalità dei fattori giustifica il passaggio dai due controlli locali al risultato sul modulo originale.

$$5 \mid (u - v)$$

$$11 \mid (u - v)$$

$$\downarrow$$

$$55 \mid (u - v)$$

$$u \equiv v \pmod{55}$$

Entrambi i primi dividono la differenza. Anche il loro prodotto la divide.

Richiami Se p, q sono primi distinti e dividono entrambi un intero w, allora $pq \mid w$. Congruenze uguali significano differenza divisibile.

La correttezza per un messaggio arbitrario

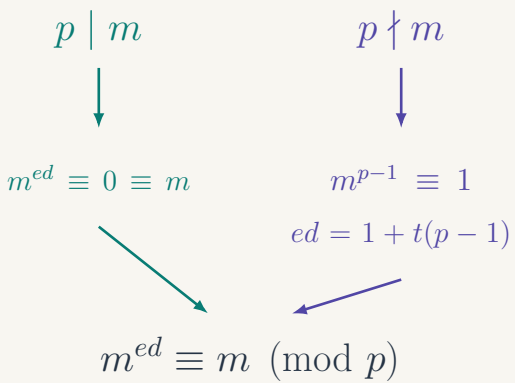
Consideriamo ora un messaggio qualunque m e un modulo $N = pq$, con primi distinti. La chiave soddisfa $ed = 1 + k(p-1)(q-1)$. Osserviamo dapprima il calcolo modulo p.

Se p divide m, il messaggio e ogni sua potenza positiva hanno resto zero, quindi $m^{ed} \equiv m$. Se p non divide m, Fermat fornisce $m^{p-1} \equiv 1$. Ponendo $t = k(q-1)$, abbiamo $ed - 1 = t(p-1)$ e otteniamo

$$m^{ed} = m\Big(m^{p-1}\Big)^t \equiv m.$$

I due casi esauriscono tutte le possibilità per un resto modulo un primo. Possiamo ripetere lo stesso ragionamento modulo q, scambiando i ruoli dei due primi. In entrambi i moduli la composizione conserva il resto del messaggio.

Un messaggio qualunque, osservato modulo p



Il ragionamento si ripete modulo q, distinguendo ancora i due possibili casi.

Richiami Fermat: se $p \nmid m$, allora $m^{p-1} \equiv 1 \pmod{p}$. La chiave impone $ed - 1 = k(p-1)(q-1)$.

Il recupero di tutti i messaggi ammessi

Dai due argomenti precedenti sappiamo che $m^{ed} - m$ è divisibile sia per p sia per q. I primi sono distinti, quindi il loro prodotto $N = pq$ divide la stessa differenza:

$$m^{ed} \equiv m \pmod{N}.$$

La riduzione finale e il messaggio iniziale appartengono all'intervallo $0 \leq m < N$. La congruenza garantisce dunque che coincidano come numeri in quell'intervallo.

La dimostrazione comprende i messaggi coprimi, i multipli di un solo fattore e il messaggio zero. Non occorre cambiare la chiave quando cambia il messaggio. La relazione $ed \equiv 1 \pmod{(p-1)(q-1)}$ garantisce il ritorno nei rami non nulli, mentre la divisibilità garantisce il ritorno nei rami nulli.

L'ipotesi che il modulo sia il prodotto di due primi distinti appartiene alla costruzione RSA qui esaminata.

Richiami RSA con $N = pq$, $p \neq q$ primi: $ed \equiv 1 \pmod{(p-1)(q-1)}$ implica $(m^e)^d \equiv m \pmod{N}$ per ogni messaggio ammesso.

Un residuo descritto mediante due resti

Nota facoltativa: connessione algebrica

Riprendi il testo: p. 110

Il teorema cinese del resto afferma che, per moduli coprimi p e q, ogni coppia di resti identifica un unico residuo modulo pq. La corrispondenza associa a x la coppia $(x \bmod p, x \bmod q)$ e conserva somme e prodotti.

Per i moduli 5 e 11, il numero 11 ha resti $(1, 0)$ e il numero 45 ha resti $(0, 1)$. Di conseguenza $11u + 45v$ ha resti (u, v). Riducendolo modulo 55, troviamo il rappresentante cercato.

Per la coppia $(0, 5)$ otteniamo $225 \bmod 55 = 5$. Questa costruzione aggiunge l'esistenza di un residuo per ogni coppia all'unicità già usata nella prova. La prova di correttezza di RSA è completa anche senza questo approfondimento.

La coppia dei resti

$$(u, v) = (0, 5)$$

$$u = x \bmod 5, \quad v = x \bmod 11$$

$$\downarrow$$

$$x = (11u + 45v) \bmod 55$$

$$(11 \cdot 0 + 45 \cdot 5) \bmod 55 = 5$$

$$11 \leftrightarrow (1, 0), \qquad 45 \leftrightarrow (0, 1)$$

Le due componenti descrivono lo stesso residuo modulo 55.

Richiami Moduli coprimi: $\gcd(p, q) = 1$. Il teorema cinese identifica i residui modulo pq con le coppie di residui modulo p e modulo q.

Le informazioni disponibili a ciascun partecipante

Il destinatario ha scelto i primi, calcolato il modulo e ricavato l'esponente privato. Può pubblicare N ed e senza pubblicare p, q e d. Il mittente usa la coppia pubblica per cifrare. Un osservatore del canale può conoscere anche il cifrato c, ma questi dati non includono direttamente la fattorizzazione.

Nel nostro esempio ogni numero è abbastanza piccolo da permettere una ricerca esaustiva. Lo scopo didattico è distinguere le operazioni e le conoscenze, non simulare una sicurezza reale. Nel seguito partiremo dai dati dell'osservatore: N, e, c. Cercheremo il periodo delle potenze di c, dal quale ricaveremo un esponente sufficiente a decifrare il messaggio. Per seguire questa via non occorre conoscere prima i fattori del modulo.

Partecipante	Dati necessari
Mittente	N, e, m
Destinatario	N, d, c
Osservatore	N, e, c

La tabella distingue i dati necessari alle operazioni. Il destinatario conosce inoltre i fattori usati per costruire il modulo e l'esponente privato.

Richiami Chiave pubblica: (N, e). Esponente privato: d, scelto con $ed \equiv 1 \pmod{\varphi(N)}$. Il cifrato è $c = m^e \bmod N$.

Fattori del modulo e periodo del cifrato

Supponiamo di ottenere la fattorizzazione del modulo pubblico $N = 55$. Dai fattori 5 e 11 ricaviamo immediatamente $\varphi(55) = 40$. L'esponente pubblico è 3, quindi possiamo ripetere Euclide esteso e calcolare l'inverso 27 modulo 40. Abbiamo così costruito un esponente che decifra i messaggi.

La fattorizzazione consente dunque di ricostruire una chiave valida per tutti i messaggi. Per decifrare il cifrato considerato seguiremo però una via più diretta. Studieremo il periodo delle potenze di c e useremo quel periodo per trovare un esponente che recuperi il messaggio. L'esponente ottenuto in questo modo non coincide necessariamente con la chiave privata universale. Il capitolo seguente mostrerà il procedimento partendo dal cifrato 13 modulo 55, mentre la fattorizzazione resterà un'applicazione conclusiva della stessa ricerca del periodo.

$$55 = 5 \cdot 11, \qquad \varphi(55) = 40, \qquad 3 \cdot 27 \equiv 1 \pmod{40}$$

Richiami Per $N = pq$, $\varphi(N) = (p-1)(q-1)$. Euclide esteso trova l'inverso di e quando $\gcd(e, \varphi(N)) = 1$.

La primitiva RSA e lo schema di cifratura

La trasformazione $m \mapsto m^e \bmod N$ è deterministica: con la stessa chiave, uno stesso messaggio produce sempre lo stesso cifrato. Inoltre il nostro racconto ha supposto che un messaggio fosse già rappresentato da un intero nel corretto intervallo. Una comunicazione reale deve affrontare anche la codifica, la casualità e le altre proprietà richieste a uno schema di cifratura.

Per questo gli esempi numerici vanno letti come studio della primitiva aritmetica RSA. La dimostrazione che decifrare annulla cifrare è necessaria, ma da sola non dimostra la sicurezza di un sistema. L'attacco che studieremo recupera il rappresentante aritmetico del messaggio a partire dal cifrato. Anche quando quel rappresentante include una codifica casualizzata, invertirne l'elevamento a potenza compromette la riservatezza: la codifica pubblica permette poi di risalire al contenuto. La costruzione di uno schema completo non elimina quindi la vulnerabilità a una ricerca efficiente del periodo.

Richiami La correttezza afferma che $c^d \bmod N = m$ dopo la cifratura. Questa proprietà aritmetica è distinta dai requisiti di sicurezza di uno schema.

Due messaggi da verificare

Conserviamo la chiave pubblica $(55, 3)$ e l'esponente privato 27. Per il messaggio 2, la cifratura dà immediatamente $2^3 = 8$. La decifratura deve quindi restituire 2 da $8^{27} \bmod 55$. Per il messaggio 10, invece, $10^3 = 1000 = 18 \cdot 55 + 10$, perciò il cifrato coincide con il messaggio.

Quest'ultimo caso non contraddice la correttezza: una trasformazione invertibile può lasciare fermi alcuni elementi. È però un ulteriore motivo per non identificare la sola trasformazione aritmetica con uno schema sicuro. Prima di leggere la soluzione, si possono calcolare i quadrati successivi di 8 e di 10, selezionando poi gli esponenti 16, 8, 2 e 1.

$$2 \longmapsto 8, \qquad 10 \longmapsto 10$$

Richiami La decifratura usa $d = 27 = 16 + 8 + 2 + 1$. Si possono ridurre modulo 55 tutte le potenze intermedie.

La verifica dei due messaggi

Per decifrare 8, i resti dei quadrati successivi sono $8, 9, 26, 16, 36$ agli esponenti $1, 2, 4, 8, 16$. Il prodotto selezionato è $36 \cdot 16 \cdot 9 \cdot 8$. Riducendo progressivamente otteniamo 26, poi 14 e infine 2. Il messaggio iniziale è dunque recuperato.

Per decifrare 10, il primo quadrato lascia resto 45. Ogni quadrato successivo conserva quel resto, perché $45^2 = 2025 \equiv 45 \pmod{55}$. Gli esponenti 16, 8 e 2 contribuiscono quindi ciascuno con 45, mentre l'esponente 1 contribuisce con 10. Il loro prodotto lascia resto 10. Abbiamo verificato anche un messaggio non coprimo, dato che $\gcd(10, 55) = 5$, senza applicare Eulero fuori dalle sue ipotesi.

$$36 \cdot 16 \cdot 9 \cdot 8 \equiv 2 \pmod{55}$$

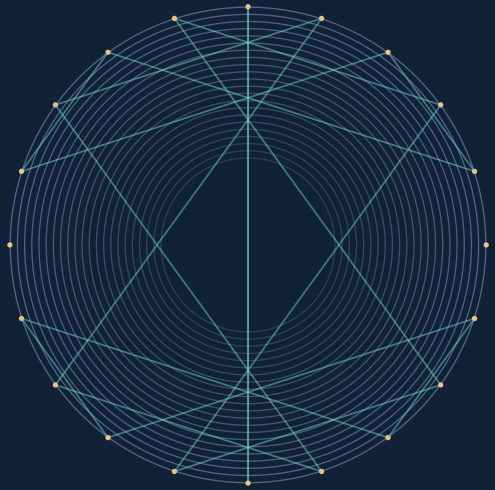
$$45 \cdot 45 \cdot 45 \cdot 10 \equiv 10 \pmod{55}$$

Richiami Per un esponente 27, si moltiplicano le potenze con esponenti $16, 8, 2, 1$. La correttezza RSA include i messaggi non coprimi.

CAPITOLO 06

Il periodo del cifrato

Il recupero del messaggio attraverso un periodo



Il cifrato come punto di partenza

Chi intercetta una comunicazione RSA conosce il modulo N, l'esponente pubblico e e il cifrato c. Il messaggio m rimane invece sconosciuto. Consideriamo un cifrato coprimo con N, come 13 modulo 55. Nel nostro esempio i dati disponibili sono $N = 55$, $e = 3$ e $c = 13$: occorre risalire al numero che, elevato al cubo e ridotto modulo 55, produce 13.

Finora abbiamo descritto la decifratura di chi possiede l'esponente privato d. Esiste tuttavia un'altra possibilità: studiare le potenze del cifrato e ricavarne un esponente sufficiente a recuperare il messaggio. Per seguire questa strada non occorre conoscere i fattori di N. Il suo punto di partenza è una funzione che possiamo già calcolare con i soli dati pubblici.

I dati del problema

$$N = 55 \qquad e = 3$$

modulo ed esponente pubblici

$$m = ? \xrightarrow{m^3 \bmod 55} c = 13$$

L'osservatore conosce 55, 3 e 13.

Il testo in chiaro m è l'incognita.

Cifratura: $c = m^e \bmod N$

Richiami Caso trattato: $\gcd(c, N) = 1$. Se $c = 0$, anche $m = 0$; se $1 < \gcd(c, N) < N$, il massimo comune divisore ha già trovato un fattore di N.

Una funzione costruita con dati pubblici

Consideriamo $f(x) = 13^x \bmod 55$, dove l'ingresso x è un esponente intero non negativo. Il valore della funzione è il resto, non l'intera potenza. In particolare, $f(0) = 1$: come per ogni base non nulla, la potenza di esponente zero vale uno.

Ogni termine successivo si ottiene moltiplicando il resto precedente per 13 e conservando nuovamente soltanto il resto modulo 55. Per esempio, dopo 13 compare 4, perché $169 = 3 \cdot 55 + 4$; dopo 4 compare 52. Questa ricorrenza evita di scrivere potenze sempre più grandi. La successione è completamente determinata e riproducibile: la sua irregolarità visiva non deriva dal caso, ma dalla riduzione modulo 55.

Potenze calcolate per ricorrenza

$$f(x+1) = 13 f(x) \bmod 55$$
$$f(0) = 1$$
$$\downarrow$$
$$13 \cdot 1 = 13 = 0 \cdot 55 + 13$$
$$f(1) = 13$$
$$\downarrow$$
$$13 \cdot 13 = 169 = 3 \cdot 55 + 4$$
$$f(2) = 4$$
$$\downarrow$$
$$13 \cdot 4 = 52 = 0 \cdot 55 + 52$$
$$f(3) = 52$$

Richiami $f(x) = c^x \bmod N$; $f(0) = 1$ e $f(x+1) = c\, f(x) \bmod N$. La variabile x è un esponente; $f(x)$ è un resto.

Il primo ritorno a uno

Proseguendo il calcolo troviamo venti resti distinti prima che ricompaia il valore iniziale. La prima ripetizione di 1 avviene per $x = 20$; da quel momento la stessa regola di moltiplicazione produce nuovamente 13, poi 4, poi 52, e così via. La successione ripercorre quindi il medesimo ciclo.

Chiamiamo periodo minimo il più piccolo intero positivo r per cui $f(x + r) = f(x)$ per ogni x. Nell'esempio vale $r = 20$. Il nastro mostra l'intero ciclo per renderne controllabile il calcolo, ma questa enumerazione serve soltanto alla spiegazione: per un modulo molto grande potrebbe richiedere un numero proibitivo di termini. Dovremo ottenere la stessa informazione senza compilare una tabella così lunga.

Il ciclo delle potenze di 13 modulo 55

Indice x in alto; resto $13^x \bmod 55$ in basso

$x = 0$ → 1	$x = 1$ → 13	$x = 2$ → 4	$x = 3$ → 52	$x = 4$ → 16
$x = 5$ → 43	$x = 6$ → 9	$x = 7$ → 7	$x = 8$ → 36	$x = 9$ → 28
$x = 10$ → 34	$x = 11$ → 2	$x = 12$ → 26	$x = 13$ → 8	$x = 14$ → 49
$x = 15$ → 32	$x = 16$ → 31	$x = 17$ → 18	$x = 18$ → 14	$x = 19$ → 17

$$x = 20 : \quad f(20) = 1 = f(0)$$

Lettura per righe: da sinistra a destra.

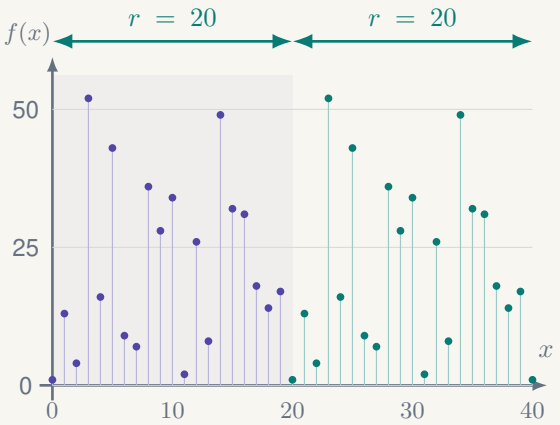
Richiami Periodo minimo: il più piccolo $r > 0$ con $f(x + r) = f(x)$ per ogni x. Per $f(x) = 13^x \bmod 55$ risulta $r = 20$.

Dal ritorno a uno alla ripetizione del ciclo

Il ritorno a uno non è soltanto un indizio grafico. Se $c^r \equiv 1 \pmod N$, allora $c^{x+r} = c^x c^r \equiv c^x \pmod N$: ogni termine riappare dopo r passi. Viceversa, se la successione ha periodo r, applicando la definizione a $x = 0$ otteniamo $c^r \equiv c^0 = 1 \pmod N$.

Le due descrizioni sono dunque equivalenti. Il periodo minimo della funzione è il più piccolo esponente positivo che riporta la potenza a uno; questo numero si chiama anche ordine di c modulo N. Nel grafico, la seconda sequenza di venti resti riproduce esattamente la prima. La coincidenza riguarda tutti i valori corrispondenti, non soltanto le estremità del ciclo.

Un andamento irregolare che si ripete



Valori interi; nessuna interpolazione.

Richiami Ordine di c modulo N: minimo $r > 0$ con $c^r \equiv 1 \pmod N$. Lavoriamo con $\gcd(c, N) = 1$, qui $\gcd(13, 55) = 1$.

Messaggio e cifrato hanno lo stesso periodo

Il periodo delle potenze del cifrato è utile perché coincide con quello delle potenze del messaggio. Per capirlo bastano le due relazioni della cifratura RSA: $c \equiv m^e \pmod N$ e $m \equiv c^d \pmod N$. La seconda relazione è vera anche quando l'osservatore non conosce il valore segreto di d.

Se $c^r \equiv 1$, elevare $m \equiv c^d$ alla potenza r mostra che anche $m^r \equiv 1$. Nell'altra direzione, ogni esponente che riporta m a uno riporta a uno anche $c = m^e$. I due insiemi di esponenti di ritorno coincidono, e quindi coincidono i rispettivi minimi. Possiamo perciò studiare il cifrato pubblico per ottenere una proprietà del messaggio ancora sconosciuto.

Le due successioni ritornano insieme

$$m \longrightarrow c = m^e$$

RSA garantisce anche
$m \equiv c^d \pmod N$.

$$c^r \equiv 1 \implies m^r \equiv (c^r)^d \equiv 1$$

$$m^t \equiv 1 \implies c^t \equiv (m^t)^e \equiv 1$$

Ogni ritorno a uno dell'una
è anche un ritorno dell'altra.

Le congruenze sono tutte modulo N.

Richiami RSA garantisce $c \equiv m^e$ e $m \equiv c^d$ modulo N. Da $c^r \equiv 1$ segue $m^r \equiv 1$, senza conoscere numericamente d.

Un esponente ricavato dal periodo

Supponiamo ora di conoscere r. Cerchiamo un intero positivo d_c per cui ed_c superi di uno un multiplo del periodo: $ed_c = 1 + kr$. In altre parole, d_c deve essere l'inverso moltiplicativo di e modulo r. Non stiamo cercando la frazione $1/e$, ma una soluzione intera a una congruenza.

Con $e = 3$ e $r = 20$ basta scegliere $d_c = 7$, perché $3 \cdot 7 = 21 = 1 + 20$. Negli esponenti, venti passi corrispondono a un giro completo; ventuno passi hanno dunque lo stesso effetto di un passo. Per una chiave RSA valida l'inverso richiesto esiste: il periodo divide $\varphi(N)$ e l'esponente pubblico è stato scelto coprimo con $\varphi(N)$, quindi anche con r.

Un giro completo e un passo

$$e\,d_c \;=\; 1 + kr$$

$$3 \cdot 7 \;=\; 1 + 20$$

20 passi: ritorno al punto iniziale



Negli esponenti, $21 \equiv 1 \pmod{20}$.

Inverso modulo r, non reciproco reale $1/e$.

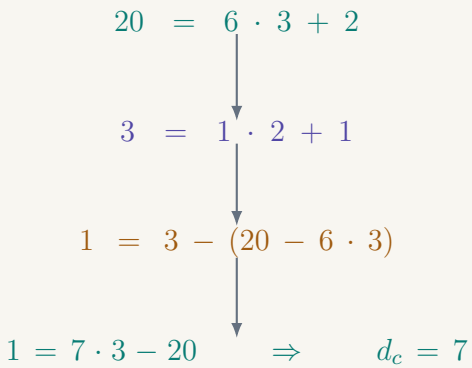
Richiami $ed_c \equiv 1 \pmod{r}$ significa $ed_c = 1 + kr$. Coprimi: massimo comune divisore uguale a 1. $\varphi(N)$ conta i resti invertibili modulo N.

Il calcolo classico dell'inverso

Il valore d_c non deve essere indovinato. L'algoritmo di Euclide trova il massimo comune divisore di e e r mediante divisioni successive; rileggendo le stesse divisioni a ritroso si ottiene una combinazione intera dei due numeri. Quando il massimo comune divisore vale uno, questa combinazione fornisce l'inverso cercato.

Nel nostro esempio dividiamo 20 per 3, ottenendo resto 2, e poi 3 per 2, ottenendo resto 1. Sostituendo la prima relazione nella seconda ricaviamo $1 = 7 \cdot 3 - 20$. Il coefficiente di 3 è dunque 7: riducendo l'uguaglianza modulo 20 rimane $3 \cdot 7 \equiv 1$. Una volta disponibile il periodo, questo passaggio si esegue efficientemente su un computer classico, anche per interi molto grandi.

L'algoritmo di Euclide, letto a ritroso



Richiami Euclide esteso produce $ue + vr = 1$ quando $\gcd(e, r) = 1$; allora $u \bmod r$ è l'inverso di e. Qui $7 \cdot 3 - 1 \cdot 20 = 1$.

Il recupero del messaggio

Dopo aver ricavato $d_c = 7$, calcoliamo $c^{d_c} \bmod N = 13^7 \bmod 55$. Anche questa operazione è classica. Non occorre costruire il grande intero 13^7: possiamo ridurre modulo 55 dopo ogni moltiplicazione, perché sostituire un fattore con un resto congruente non cambia il resto finale.

Poiché $7 = 4 + 2 + 1$, ci bastano 13^4, 13^2 e 13. I loro resti sono rispettivamente 16, 4 e 13; il prodotto vale 832, il cui resto modulo 55 è 7. Abbiamo quindi recuperato il messaggio $m = 7$. La verifica conclusiva ripercorre la cifratura pubblica: $7^3 = 343 = 6 \cdot 55 + 13$. Il risultato restituisce proprio il cifrato intercettato e chiude il calcolo senza utilizzare i fattori del modulo.

La decifratura richiede solo aritmetica classica

$$13^2 = 169 \equiv 4 \pmod{55}$$

$$\downarrow$$

$$13^4 \equiv 4^2 = 16 \pmod{55}$$

$$\downarrow$$

$$13^7 = 13^{4+2+1} \equiv 16 \cdot 4 \cdot 13$$

$$\downarrow$$

$$832 = 15 \cdot 55 + 7 \quad \Rightarrow \quad m = 7$$

Richiami Decifratura dal periodo: $m = c^{d_c} \bmod N$. Qui $d_c = 7$ e $13^7 \bmod 55 = 7$; verifica: $7^3 \bmod 55 = 13$.

L'identità che rende possibile la decifratura

Il calcolo precedente non dipende da una coincidenza dei piccoli numeri scelti. Sostituiamo $c \equiv m^e$ nella potenza che intendiamo calcolare: otteniamo $c^{d_c} \equiv m^{ed_c}$. La scelta dell'inverso modulo r trasforma l'esponente in $1 + kr$, per cui il risultato diventa m moltiplicato per k potenze di m^r.

Abbiamo già stabilito che $m^r \equiv 1 \pmod{N}$. Tutti questi fattori aggiuntivi sono quindi uguali a uno nell'aritmetica modulare e rimane soltanto m. Il ruolo del periodo è precisamente questo: identifica incrementi dell'esponente che non alterano il valore della potenza. L'inverso d_c sfrutta tale ripetizione per trasformare l'esponente di cifratura in un singolo passo, restituendo il messaggio originale.

L'identità che restituisce il messaggio

$$c \equiv m^e \pmod{N}$$

$$\downarrow$$

$$c^{d_c} \equiv m^{ed_c} = m^{1+kr}$$

$$\downarrow$$

$$m^{1+kr} = m\,(m^r)^k$$

$$\downarrow$$

$$m^r \equiv 1 \quad \Rightarrow \quad c^{d_c} \equiv m$$

Richiami Relazioni utilizzate: $c \equiv m^e$, $m^r \equiv 1$, $ed_c = 1 + kr$. Ne segue $c^{d_c} \equiv m(m^r)^k \equiv m \pmod{N}$.

Decifrare un cifrato e ricostruire una chiave

L'esponente privato d e l'esponente d_c ottenuto dal periodo soddisfano condizioni diverse. Il primo viene scelto per la chiave RSA; il secondo è ricavato dall'ordine del cifrato osservato. Il procedimento appena descritto garantisce la decifratura di quel cifrato, senza richiedere la ricostruzione dell'esponente privato originario.

Nel caso principale $d = 27$ e $d_c = 7$ funzionano entrambi; qui anche 7 funziona per tutti i messaggi, ma non è una garanzia generale del metodo. Con la stessa chiave, il cifrato 26 ha periodo 5: l'inverso di 3 modulo 5 è 2, e $26^2 \bmod 55 = 16$ recupera il suo messaggio. Applicare però 2 al nostro cifrato 13 darebbe 4, non 7.

Due esponenti con condizioni diverse

Esponente privato d

$$ed \equiv 1 \pmod{\varphi(N)}$$

Per la chiave dell'esempio:

$$3 \cdot 27 = 81 \equiv 1 \pmod{40}.$$

Esponente ricavato dal cifrato d_c

$$ed_c \equiv 1 \pmod{r}$$

Per $c = 13$: $3 \cdot 7 = 21 \equiv 1 \pmod{20}$.

r riguarda le potenze del cifrato osservato.

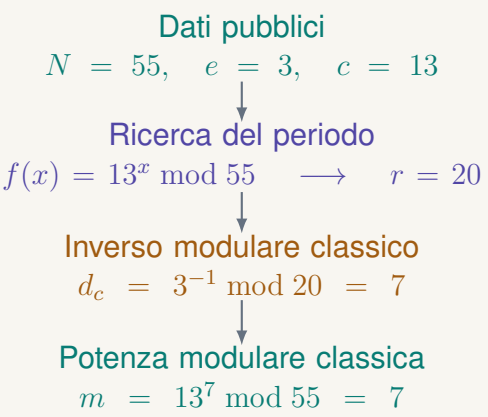
Richiami d riguarda l'intera chiave; $d_c = e^{-1} \bmod r$ è sufficiente per il cifrato di ordine r. I due esponenti non vanno identificati.

La ricerca del periodo basta a decifrare

Possiamo ora riassumere il procedimento dal punto di vista di chi dispone soltanto dei dati pubblici. Dal cifrato c e dal modulo N si definisce la funzione $f(x) = c^x \bmod N$. Se una procedura ne determina il periodo minimo r, il resto del lavoro consiste in due calcoli classici: trovare l'inverso di e modulo r ed eseguire una potenza modulare.

Il diagramma distingue questi passaggi senza inserire la fattorizzazione come intermediario. Conoscere i fattori consentirebbe certamente di ricostruire una chiave privata, ma non è la strada necessaria per il risultato ottenuto qui. L'informazione nuova che rende possibile la decifratura è il periodo delle potenze del cifrato. Sarà quindi la ricerca di quel periodo, e non il calcolo dell'inverso, a richiedere l'algoritmo quantistico.

La sola informazione mancante è il periodo



Richiami Dati pubblici (N, e, c); funzione $f(x) = c^x \bmod N$; periodo r; inverso $d_c = e^{-1} \bmod r$; messaggio $m = c^{d_c} \bmod N$.

Il problema rimasto aperto

Fin qui abbiamo dimostrato una conseguenza condizionata: se il periodo è disponibile, possiamo decifrare. Nel piccolo esempio abbiamo trovato $r = 20$ percorrendo tutta la successione, ma questa tabella non costituisce ancora un algoritmo efficiente per moduli di dimensione crittografica. Il fatto che una funzione sia periodica non implica che il suo periodo si possa leggere da pochi valori.

Occorre dunque separare due compiti. Calcolare $f(x)$ per un esponente assegnato è un'operazione accessibile; ricostruire il minimo intervallo dopo cui tutti i valori si ripetono è un problema diverso. Prima di introdurre Fourier esamineremo questa differenza, così che il lettore sappia quale informazione stiamo cercando e quale difficoltà la trasformata dovrà aiutarci a superare.

Il risultato raggiunto e il problema ancora aperto

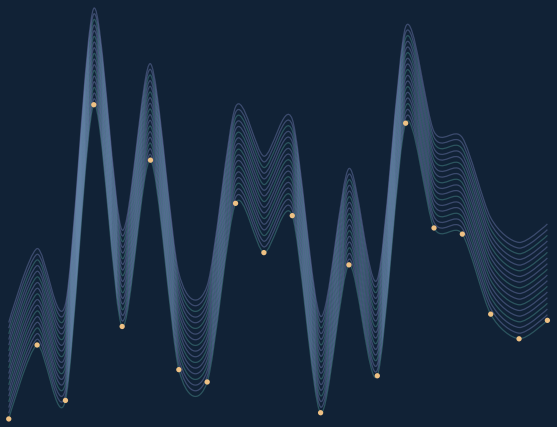
$$r \text{ noto}$$
$$\downarrow$$
$$d_c = e^{-1} \bmod r$$
$$\downarrow$$
$$m = c^{d_c} \bmod N$$

Trovare r senza enumerare il ciclo.

Richiami La conclusione ottenuta è: periodo noto $\Rightarrow$ decifratura efficiente. Rimane da determinare r senza enumerare necessariamente tutti i suoi termini.

CAPITOLO 07

La difficoltà della ricerca



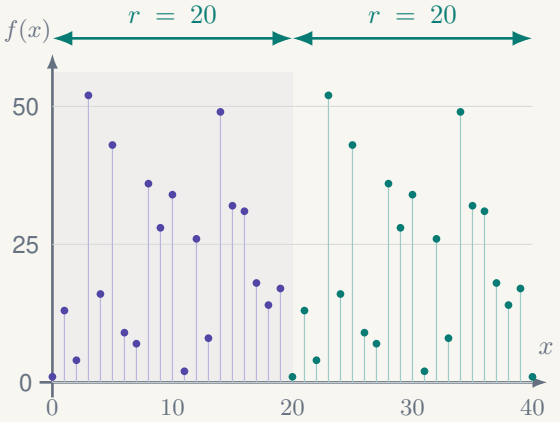
Valutare una potenza e determinare il suo periodo

Una ripetizione priva di andamento regolare

Una funzione periodica viene spesso immaginata come una sinusoide: una curva che sale e scende gradualmente, rendendo riconoscibile la durata di un'oscillazione. Le potenze modulari hanno una struttura diversa. I valori $1, 13, 4, 52, 16, \ldots$ si succedono senza una crescita o una discesa regolare; la ripetizione riguarda l'intera sequenza, non un profilo deducibile dai primi punti.

Nel grafico riconosciamo il periodo 20 perché sono mostrati due cicli completi. Questa informazione ha però un costo: sono stati calcolati tutti i punti. Se il periodo fosse enorme, pochi campioni isolati non offrirebbero necessariamente lo stesso indizio. Occorre ottenere il periodo senza dover prima costruire l'intero grafico.

Un andamento irregolare che si ripete



Valori interi; nessuna interpolazione.

Richiami Periodicità: $f(x+r) = f(x)$. Non implica continuità, andamento sinusoidale o variazioni piccole tra $f(x)$ e $f(x+1)$.

Le potenze e i loro resti

Prima della riduzione, le potenze $1, 13, 169, 2197, 28561, \ldots$ crescono rapidamente e in modo prevedibile. Dopo la divisione per 55 conserviamo soltanto i resti: $1, 13, 4, 52, 16, \ldots$. I multipli interi del modulo vengono eliminati, così che una crescita molto grande della potenza può produrre un resto piccolo oppure grande, senza un andamento locale monotono.

Questo spiega l'aspetto irregolare della successione, ma non dimostra una difficoltà computazionale. Esistono periodi modulari brevi e facili da trovare, come il nostro. La difficoltà riguarda il problema generale su interi grandi: la formula consente di calcolare ogni valore, ma non fornisce automaticamente un procedimento efficiente per ricavarne il periodo minimo.

Il modulo cambia l'andamento della successione

Potenza 13^x		Resto modulo 55
1	$\longrightarrow$	1
13	$\longrightarrow$	13
169	$\longrightarrow$	4
$2\,197$	$\longrightarrow$	52
$28\,561$	$\longrightarrow$	16

Ogni riga conserva solo il resto della divisione per 55.

Richiami Scrivere $a \bmod N$ significa conservare s nell'uguaglianza $a = qN + s$, con $0 \leq s < N$. Il modulo non rende difficile ogni singolo caso.

Una potenza assegnata si calcola rapidamente

Per valutare $f(37)$ non dobbiamo moltiplicare 13 per sé stesso trentasette volte. Scriviamo invece $37 = 32 + 4 + 1$ e costruiamo le potenze con esponenti $1, 2, 4, 8, 16, 32$ mediante elevamenti al quadrato successivi. A ogni passaggio riduciamo il risultato modulo 55, mantenendo piccoli gli interi memorizzati.

Nel diagramma i tre resti selezionati sono $13^{32} \equiv 26$, $13^4 \equiv 16$ e $13^1 \equiv 13$; il loro prodotto, ridotto modulo 55, vale 18. In generale il numero di quadrati e moltiplicazioni cresce con il numero di bit dell'esponente, non con il suo valore. Conoscere rapidamente $f(37)$ non rivela però dove si trovi il primo ritorno a uno. La valutazione di una funzione e la ricerca del suo periodo rimangono compiti distinti.

Quadrati successivi per un esponente assegnato

$$37 = 32 + 4 + 1$$

$$13^1 \bmod 55 = 13$$
$$13^2 \bmod 55 = 4$$
$$13^4 \bmod 55 = 16$$
$$13^8 \bmod 55 = 36$$
$$13^{16} \bmod 55 = 31$$
$$13^{32} \bmod 55 = 26$$

$$13^{37} \equiv 26 \cdot 16 \cdot 13 \equiv 18 \pmod{55}$$

5 quadrati successivi e 2 moltiplicazioni.

Richiami Esponenziazione modulare: scomporre x in potenze di 2, calcolare quadrati successivi e moltiplicare i fattori selezionati. Qui $13^{37} \bmod 55 = 18$.

Il costo va misurato nel numero di bit

Per scrivere N in binario bastano circa $\log_2 N$ bit. Un algoritmo efficiente deve quindi richiedere un tempo controllato da una potenza del numero di bit, non semplicemente da una potenza del valore numerico di N.

Una scansione fino al primo ritorno a uno eseguirebbe circa r valutazioni. Poiché i periodi possono essere molto grandi, questa procedura può diventare impraticabile all'aumentare della lunghezza della chiave. La tabella mostra quanto rapidamente cresce lo spazio dei valori quando aumentano i bit: non dimostra che ogni algoritmo debba esplorarlo tutto. Esistono metodi classici migliori della scansione, ma non è noto un algoritmo classico generale polinomiale per questo problema.

La dimensione dell'ingresso
è il numero di bit

$$n_0 = \lceil \log_2 N \rceil$$

n_0	2^{n_0}
10	1 024
20	1 048 576
40	1 099 511 627 776

Pochi bit in più,
molti più valori possibili.

Confronto di dimensioni, non di algoritmi.

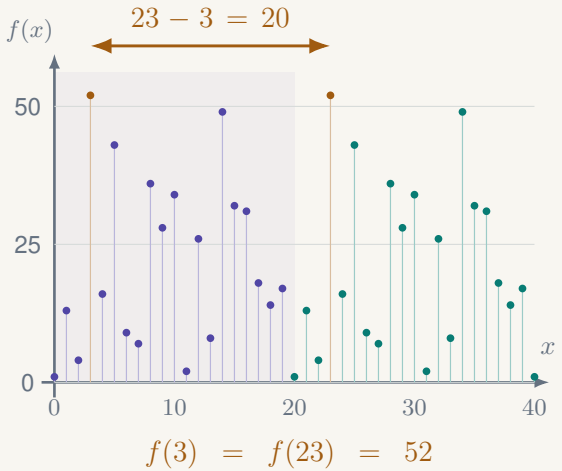
Richiami Dimensione dell'ingresso: $n_0 = \lceil \log_2 N \rceil$. Un costo polinomiale è limitato da $O(n_0^k)$ per una costante k; $O(N)$ non è polinomiale in n_0.

Due valori uguali rivelano una distanza utile

Possiamo calcolare la funzione su diversi ingressi finché due risultati coincidono. Nell'esempio $f(3) = f(23) = 52$: la differenza $23 - 3 = 20$ individua il periodo. In generale una coincidenza restituisce un multiplo del periodo, non necessariamente il suo valore minimo; occorrono quindi altri controlli.

Quando il ciclo contiene moltissimi resti distinti, il campionamento casuale può richiedere una grande raccolta di valori prima di incontrare una ripetizione. Questo limite non dimostra l'impossibilità di ogni algoritmo classico. Chiarisce invece l'obiettivo del procedimento quantistico: ottenere informazione sulla distanza tra le ripetizioni senza aspettare di osservare direttamente due esponenti con lo stesso resto. La raccolta stessa dei campioni può essere proibitiva.

Un andamento irregolare che si ripete



Richiami Con $\gcd(c, N) = 1$, $f(x) = f(y)$ equivale a $x - y$ multiplo di r. Una collisione è una coppia di ingressi distinti con lo stesso valore.

Il limite dei procedimenti classici noti

La scansione delle potenze e il campionamento casuale non esauriscono le possibilità classiche. Esistono algoritmi che sfruttano proprietà aritmetiche più profonde e migliorano su queste strategie. Il confronto con un algoritmo quantistico deve tener conto di tali metodi, non soltanto dell'enumerazione più semplice.

Per la ricerca generale dell'ordine non è tuttavia noto un algoritmo classico polinomiale nella lunghezza binaria degli ingressi. È un'affermazione sulle conoscenze disponibili, non la dimostrazione che un simile algoritmo non possa esistere. Shor fornisce invece una procedura quantistica polinomiale, includendo preparazione dei dati e calcoli classici necessari a interpretare la misura.

Una distinzione sul costo degli algoritmi

Enumerare tutte le potenze

Non coincide con il miglior procedimento classico.

Algoritmi classici generali noti

Oltre la scansione, ma non polinomiali nei bit.

Assenza di un algoritmo noto

non significa impossibilità matematica dimostrata

Richiami *Non noto* e *impossibile* non sono sinonimi. Il confronto dei costi riguarda algoritmi generali e include valutazione della funzione e interpretazione dell'esito.

Da Simon alla periodicità degli interi

Il collegamento con Simon riguarda la forma dell'informazione cercata. In quel problema due ingressi producono lo stesso valore quando differiscono per una maschera binaria nascosta: la relazione è $f(x) = f(x \oplus s)$. L'operazione che collega gli ingressi è lo XOR, eseguito bit per bit senza riporto.

Nelle potenze modulari la ripetizione segue invece l'addizione ordinaria: gli ingressi x, $x + r$, $x + 2r$ producono lo stesso resto. Per esempio, 3, 23 e 43 danno tutti 52. Cambia quindi la struttura della traslazione e non possiamo trasferire meccanicamente il calcolo svolto per Simon. Rimane però la stessa idea: usare le relazioni tra molti ingressi per ricavare una proprietà globale, anziché leggere separatamente tutti i valori della funzione.

Due forme diverse di periodicità

Simon: traslazione mediante XOR

$$010 \longleftrightarrow 111$$

$$010 \oplus 101 = 111$$

Shor: traslazione mediante somma

$$3 \xrightarrow{+20} 23 \xrightarrow{+20} 43$$

$$f(3) = f(23) = f(43) = 52$$

Ricavare la simmetria nascosta della funzione.

Richiami Simon: $x \mapsto x \oplus s$ con XOR binario. Ricerca del periodo: $x \mapsto x + r$ con somma ordinaria. Le due operazioni hanno strutture diverse.

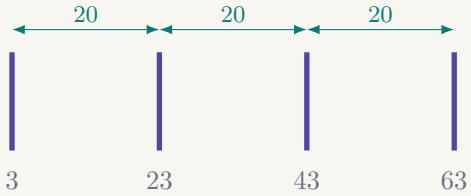
Una descrizione adatta a riconoscere le ripetizioni

Il periodo è una distanza tra ingressi: non dipende da quale ripetizione abbiamo scelto come prima. Se i punti 3, 23, 43 e 63 producono lo stesso valore, spostare tutta questa sequenza cambia la posizione iniziale, ma non la separazione di venti passi che vogliamo conoscere.

La descrizione mediante frequenze è particolarmente adatta a separare queste due informazioni. Prima di introdurre la trasformata quantistica, costruiremo perciò il significato di una componente oscillante e mostreremo come più oscillazioni possano rappresentare un andamento periodico anche molto irregolare. Partiremo da successioni piccole, con grafici e somme verificabili. Solo dopo passeremo alle ampiezze di uno stato quantistico, distinguendo con cura la trasformazione dello stato dalla lettura dei suoi risultati attraverso la misura.

Dalla distanza tra ripetizioni alle frequenze

Indici con lo stesso valore



La distanza non dipende dall'indice iniziale.

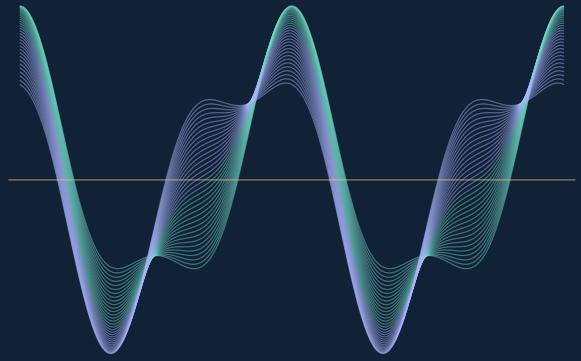
Fourier descrive la successione mediante componenti oscillanti.

Prima le frequenze, poi gli stati quantistici.

Richiami Il periodo r misura la distanza tra ripetizioni; l'offset x_0 indica dove cade la prima. Qui $x_0 = 3$ e $r = 20$ sono informazioni diverse.

CAPITOLO 08

La rappresentazione di Fourier



Oscillazioni, campioni e frequenze

Il periodo nella descrizione di una funzione

Una funzione periodica ripete gli stessi valori quando l'argomento aumenta di una quantità fissa. Nel grafico, la curva fra 0 e 4 ricompare fra 4 e 8: conoscere un tratto lungo quattro unità basta dunque a descrivere tutte le ripetizioni successive.

Il periodo fondamentale T è la più piccola traslazione positiva che lascia invariata la funzione. La frequenza fondamentale $\nu_0 = 1/T$ esprime la stessa informazione come numero di ripetizioni per unità: qui $T = 4$ e $\nu_0 = 1/4$.

Fourier propone una descrizione diversa della curva: individuare le oscillazioni semplici che, sommate, la producono. Studieremo dapprima una funzione esplicita, per capire questa rappresentazione senza introdurre ancora registri o misure quantistiche.

La forma ritorna dopo quattro unità



$$g(t+4) = g(t)$$

Un periodo lungo 4: frequenza fondamentale $1/4$.

Richiami $g(t+T) = g(t)$ definisce un periodo; il periodo fondamentale è il più piccolo $T > 0$. La frequenza corrispondente è $\nu_0 = 1/T$.

La fondamentale e le armoniche

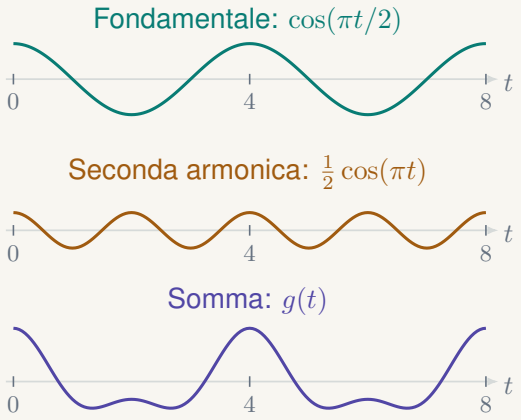
Consideriamo una curva ottenuta sommando due coseni:

$$g(t) = \cos(\pi t/2) + \tfrac{1}{2}\cos(\pi t).$$

Il primo compie un'oscillazione ogni quattro unità; il secondo ne compie due nello stesso intervallo. Le frequenze sono quindi $1/4$ e $2/4$. Chiamiamo armoniche le oscillazioni la cui frequenza è un multiplo intero della fondamentale: il secondo termine è la seconda armonica.

Il fattore $1/2$ ne riduce l'ampiezza, senza modificarne la frequenza. La somma si costruisce aggiungendo le ordinate delle due curve nello stesso punto: per esempio, in $t = 0$ si ottiene $1 + 1/2 = 3/2$. Il profilo cambia rispetto al primo coseno, ma continua a ripetersi ogni quattro unità.

Due oscillazioni, una curva composta



Richiami Per una fondamentale $1/T$, l'armonica k ha frequenza k/T e periodo T/k. L'ampiezza ne determina il contributo verticale, non il periodo.

I coefficienti della serie di Fourier

Una serie di Fourier descrive una funzione periodica mediante una componente costante e una somma di seni e coseni. Per le funzioni regolari qui considerate,

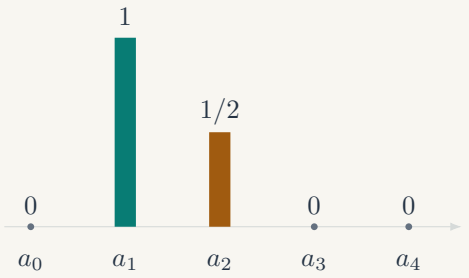
$$g(t) = a_0 + \sum_{k \geq 1} \left[a_k \cos \frac{2\pi k t}{T} + b_k \sin \frac{2\pi k t}{T} \right].$$

Ogni coefficiente indica quanto pesa una componente. Nella convenzione scritta, a_0 è il valore medio; i seni permettono di descrivere oscillazioni che non hanno un massimo nell'origine. Uno zero segnala semplicemente l'assenza di quella componente.

Nel nostro esempio, soltanto $a_1 = 1$ e $a_2 = 1/2$ sono diversi da zero. La curva, che richiede molti punti per essere disegnata, è quindi descritta esattamente da due coefficienti e dal periodo $T = 4$.

I coefficienti descrivono la composizione

Ampiezza delle componenti coseno



$a_0 = 0$, $b_k = 0$ per ogni k

Uno zero segnala una componente assente.

Richiami Qui la componente costante è a_0, non $a_0/2$: è una convenzione esplicita. Per $g(t)$: $a_1 = 1$, $a_2 = 1/2$, tutti gli altri coefficienti nulli.

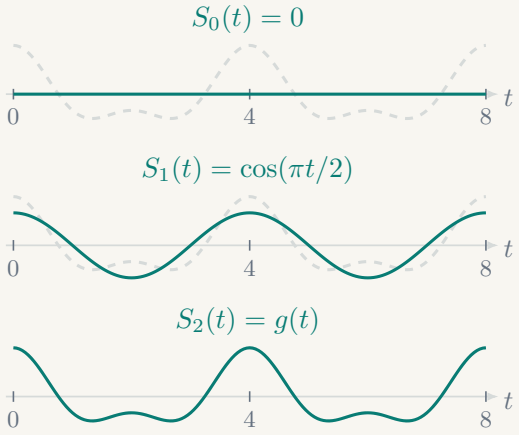
La ricostruzione della curva dalle componenti

Leggere la curva e leggere i coefficienti sono due modi di descrivere lo stesso oggetto. Per tornare dai coefficienti al grafico, si sommano le oscillazioni associate, rispettandone ampiezza e fase. Il disegno mostra questa ricostruzione per approssimazioni successive.

La sola componente costante dà $S_0(t) = 0$. Aggiungendo la fondamentale si ottiene $S_1(t) = \cos(\pi t/2)$: il periodo è già corretto, ma il profilo non coincide ancora con quello cercato. La seconda armonica corregge gli scarti e produce esattamente $S_2(t) = g(t)$.

Per una funzione generica possono servire molte componenti; qui ne bastano due perché abbiamo scelto un esempio controllabile. La rappresentazione di Fourier non è dunque un nuovo segnale: rende esplicita la composizione di quello iniziale.

La ricostruzione per somme successive



Richiami S_K è la somma fino all'armonica K. In questo esempio $S_2 = g$ esattamente; il tratteggio indica sempre la curva finale da ricostruire.

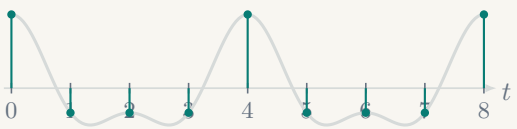
Dalla curva a una successione finita

Un calcolatore non memorizza infiniti valori di una curva. Possiamo invece registrarne i campioni, cioè i valori in posizioni scelte. Qui prendiamo $g(0), g(1), \ldots, g(31)$: sono $Q = 32$ numeri, indicizzati da $x = 0$ a $x = 31$.

I primi quattro sono $1{,}5, -0{,}5, -0{,}5, -0{,}5$; i successivi ripetono lo stesso blocco. La distanza fra due ripetizioni è di quattro indici. L'unità orizzontale è un passo fra campioni, non necessariamente un secondo.

La trasformata discreta di Fourier, o DFT, descriverà precisamente questi trentadue numeri. Non ricostruisce automaticamente ogni dettaglio della curva fra un campione e l'altro: curve diverse possono condividere gli stessi valori campionati. Il nostro problema diventa finito e dichiarato.

Una curva e i suoi valori interi



$$g(0), g(1), g(2), g(3)$$
$$1{,}5, \quad -0{,}5, \quad -0{,}5, \quad -0{,}5$$

Il blocco si ripete ogni quattro indici.

32 campioni: $x = 0, \ldots, 31$.

Richiami Un campione è un valore della funzione in una posizione scelta. Q conta i campioni; x ne indica la posizione. La DFT opera sull'intero elenco finito.

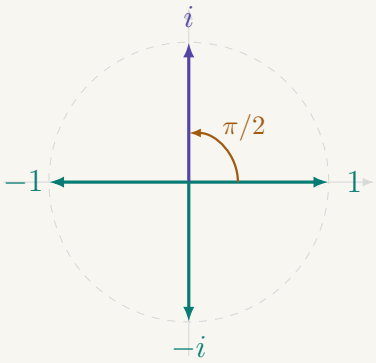
Le oscillazioni come frecce nel piano

Per descrivere insieme seni e coseni conviene usare i numeri complessi. La scrittura $z = a + ib$ rappresenta una freccia con componente orizzontale a e verticale b, dove $i^2 = -1$. Il modulo è la lunghezza della freccia; la fase ne specifica la direzione.

La formula di Eulero, riportata nel diagramma, descrive una freccia di lunghezza uno che ruota al variare di θ. A un quarto di giro corrisponde i, a mezzo giro -1 e a tre quarti $-i$. Moltiplicare per $e^{i\theta}$ equivale a ruotare di θ.

Sommare numeri complessi significa sommare le loro frecce. Due contributi opposti si annullano; due concordi si rafforzano. Questa semplice geometria spiegherà la selezione delle frequenze.

Un numero complesso come freccia



$$e^{i\theta} = \cos\theta + i\sin\theta$$

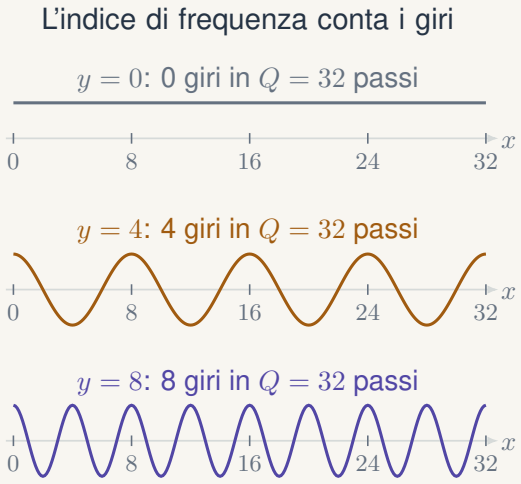
Richiami $e^{i\theta} = \cos\theta + i\sin\theta$ ha modulo 1. Somma: composizione delle frecce. Prodotto per $e^{i\theta}$: rotazione di angolo θ.

Le frequenze ammesse su trentadue campioni

Su una finestra di Q campioni scegliamo oscillazioni che completano un numero intero di giri. L'indice y conta quei giri: fra un campione e il successivo, la freccia ruota di $2\pi y/Q$. Per $Q = 32$, sono sufficienti gli indici $y = 0, \ldots, 31$.

Con $y = 0$ la freccia rimane ferma: è la componente costante. Con $y = 4$ compie quattro giri in trentadue passi; con $y = 8$ ne compie otto e ritrova la direzione iniziale ogni quattro passi.

Il diagramma mostra la componente reale delle oscillazioni, cioè il coseno. Il rapporto fra distanza e frequenza è già visibile: una ripetizione ogni quattro campioni corrisponde all'indice $y = Q/4 = 8$. Dovremo però esaminare anche le altre armoniche.



Richiami y è un indice intero di frequenza; la frequenza in cicli per campione è y/Q. Se y divide Q, una rotazione completa richiede Q/y passi.

Il coefficiente di una frequenza

Nella DFT ogni campione $u(x)$ viene ruotato di un angolo proporzionale alla sua posizione; i contributi si sommano:

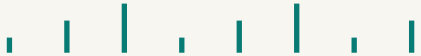
$$\widehat{u}(y) = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} u(x) e^{2\pi i x y / Q}.$$

Adottiamo il segno positivo nell'esponente; l'inversa userà quello negativo. La formula proietta sulla corrispondente oscillazione complessa di segno opposto: contributi concordi si rafforzano, direzioni diverse possono cancellarsi.

Il calcolo per ogni y produce Q coefficienti, chiamati complessivamente spettro. Il fattore $1/\sqrt{Q}$ conserva la somma dei moduli al quadrato: ritroveremo questa convenzione nel calcolo quantistico.

Una frequenza alla volta

Campioni $u(0), \ldots, u(31)$



↓

Rotazione del campione x di $2\pi x y/32$

↓

Somma e fattore $1/\sqrt{32}$

Un coefficiente complesso: $\widehat{u}(y)$

Richiami $\widehat{u}(y)$ è un numero complesso, non una frequenza. y identifica la frequenza. Con questa normalizzazione, $\sum_y |\widehat{u}(y)|^2 = \sum_x |u(x)|^2$.

Una successione con un impulso ogni quattro passi

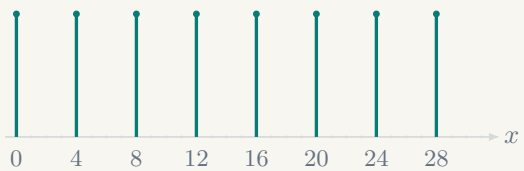
Passiamo a una successione più vicina al problema del periodo: vale zero quasi ovunque e presenta impulsi identici a distanza regolare. Con $Q = 32$ e $r = 4$, gli indici non nulli sono $0, 4, 8, 12, 16, 20, 24, 28$.

Assegniamo a ciascun impulso il valore $1/\sqrt{8}$. Questa scelta non modifica la distanza fra gli impulsi; rende uguale a uno la somma dei quadrati degli otto valori. Chiameremo $h(x)$ la successione così normalizzata.

Il periodo è immediatamente visibile se possediamo l'elenco completo. Cerchiamo ora come viene rappresentato nello spettro, perché in seguito non avremo accesso diretto a tutti i campioni. Abbiamo scelto intenzionalmente un caso esatto: quattro divide trentadue, quindi la finestra contiene otto periodi completi.

Otto impulsi equidistanti

$h(x) = 1/\sqrt{8}$ sui multipli di 4



$$8\left(1/\sqrt{8}\right)^2 = 1$$

Qui il disegno è periodico anche sul bordo: dopo l'indice 31 si ritorna all'indice 0.

Richiami $h(x) = 1/\sqrt{8}$ per $x \equiv 0 \pmod 4$, altrimenti 0. La finestra contiene $Q/r = 8$ impulsi. Qui la periodicità è compatibile con la chiusura ciclica.

Le frequenze compatibili si rafforzano

Nella DFT di h sopravvivono soltanto gli otto termini con $x = 4k$. Sostituendo nella definizione si ottiene

$$\widehat{h}(y) = \frac{1}{16} \sum_{k=0}^{7} e^{2\pi i k y/8}.$$

Per $y = 8$, ogni esponente descrive un numero intero di giri: tutte le frecce puntano verso 1, la somma vale otto e il coefficiente è $1/2$. Lo stesso accade per $y = 0, 16, 24$.

Con $y = 4$, invece, le direzioni alternano 1 e -1, cancellandosi a coppie. Con $y = 1$ formano un poligono chiuso: anche qui la somma è zero. Le restanti frequenze non compatibili si annullano nello stesso modo. I picchi nascono dunque dalla geometria della somma, non dal riconoscimento visivo del grafico.

La rotazione fra impulsi

$y = 8$: allineamento



$y = 4$: cancellazione a coppie



$y = 1$: poligono chiuso



Richiami Fra due impulsi consecutivi la rotazione è $2\pi r y/Q$. Per $r = 4$, $Q = 32$, l'allineamento avviene quando y è multiplo di 8.

La periodicità diventa una spaziatura nello spettro

Il risultato completo contiene soltanto quattro coefficienti non nulli: $\widehat{h}(0) = \widehat{h}(8) = \widehat{h}(16) = \widehat{h}(24) = 1/2$. Tutti gli altri sono zero. Nel diagramma, la successione iniziale e il suo spettro condividono la stessa scala orizzontale, ma gli assi rappresentano grandezze diverse.

In alto si leggono posizioni, separate da $r = 4$; in basso si leggono indici di frequenza, separati da $Q/r = 8$. La componente $y = 0$ è sempre presente perché gli impulsi hanno media positiva: da sola, però, non identifica il periodo.

Anche i pesi spettrali sono immediati: ciascun coefficiente contribuisce con $|1/2|^2 = 1/4$, e i quattro pesi sommano a uno. Per ora descrivono lo spettro; il loro significato nella misura quantistica verrà introdotto nel prossimo capitolo.

Il periodo seleziona quattro frequenze



Quattro coefficienti di valore $1/2$; tutti gli altri nulli.

Richiami Posizioni: $x = 0, 4, \ldots, 28$. Frequenze: $y = 0, 8, 16, 24$. Coefficiente non nullo: $1/2$; modulo al quadrato: $1/4$.

Una traslazione conserva i pesi delle frequenze

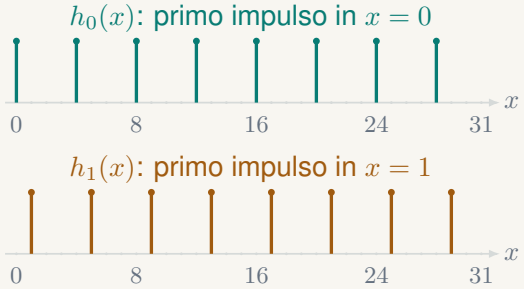
Trasliamo di una posizione tutti gli impulsi: si trovano in $1, 5, 9, \ldots, 29$. Il periodo resta quattro. Indichiamo con h_0 il pettine originale e con h_1 quello traslato.

$$\widehat{h}_1(y) = e^{2\pi i y/32}\widehat{h}_0(y).$$

La trasformata acquista una rotazione diversa per ciascuna frequenza. Nei quattro punti non nulli, i fattori sono $1, i, -1, -i$: cambiano le direzioni dei coefficienti, non il modulo $1/2$.

Un'origine sconosciuta può impedire di confrontare due posizioni osservate; i pesi dello spettro, invece, non cambiano e conservano l'informazione sul periodo. La fase non è comune all'intero spettro: dipende da y.

Lo spostamento modifica le fasi



$y = 0$	$y = 8$	$y = 16$	$y = 24$
$\times 1$	$\times i$	$\times -1$	$\times -i$

Fattori di modulo 1: $|\widehat{h}_1(y)| = |\widehat{h}_0(y)|$.

Richiami Con segno positivo nella DFT, uno spostamento di x_0 moltiplica il coefficiente y per $e^{2\pi i x_0 y/Q}$. Il modulo resta invariato.

Dalle quattro frequenze agli impulsi iniziali

Per ricostruire ogni campione dai coefficienti basta cambiare il segno dell'esponente, mantenendo il fattore di normalizzazione:

$$u(x) = \frac{1}{\sqrt{Q}} \sum_{y=0}^{Q-1} \widehat{u}(y) e^{-2\pi i x y / Q}.$$

Nel nostro pettine occorrono soltanto i quattro coefficienti non nulli. Per $x = 0$, le quattro frecce sono concordi e producono $4/(2\sqrt{32}) = 1/\sqrt{8}$. Per $x = 1$, puntano nelle quattro direzioni cardinali e si annullano. Lo stesso ragionamento vale per gli altri indici.

Gli impulsi non sono stati eliminati né approssimati: l'informazione è riscritta in una base nella quale la regolarità delle distanze assume una forma semplice.

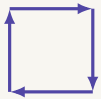
La ricostruzione del pettine

$x = 0$: quattro contributi concordi



$$h(0) = 1/\sqrt{8}$$

$x = 1$: quattro contributi si annullano



$$h(1) = 0$$

Richiami DFT diretta: esponente $+2\pi i x y/Q$. DFT inversa: esponente $-2\pi i x y/Q$. Entrambe usano $1/\sqrt{Q}$; nessuna informazione viene persa.

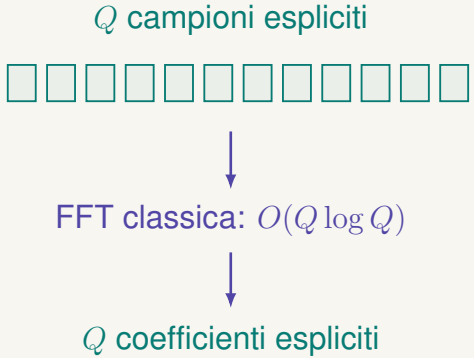
Il costo di uno spettro classico completo

La DFT spiega dove si manifesta il periodo, ma non fornisce ancora un algoritmo efficiente per RSA. Se costruiamo esplicitamente un elenco di Q campioni, dobbiamo prima ottenerli e memorizzarli. Lo spettro completo contiene a sua volta Q coefficienti.

La FFT è un algoritmo classico che calcola questo spettro in $O(Q \log Q)$ operazioni aritmetiche, invece delle $O(Q^2)$ della formula diretta. Il miglioramento è notevole, ma se $Q = 2^n$ l'elenco rimane esponenziale rispetto a n.

Nel seguito cambierà quindi l'accesso all'informazione, non la matematica di Fourier. Dovremo ottenere indizi sul periodo senza leggere tutti i valori della funzione né tutti i coefficienti. La stabilità dei pesi rispetto alla traslazione è il risultato che portiamo con noi.

Un cambiamento di rappresentazione



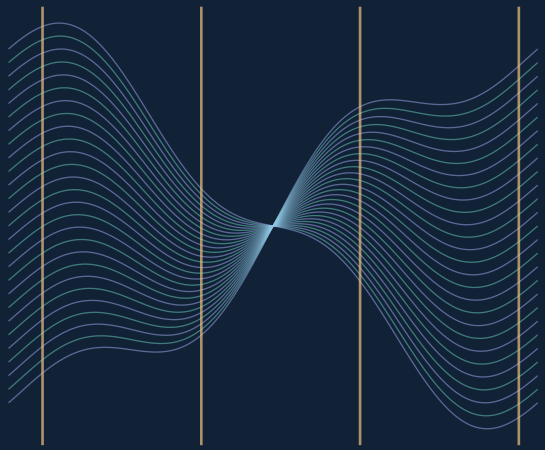
Con $Q = 2^n$, l'elenco contiene 2^n numeri.

Richiami La FFT calcola una DFT classica completa; il suo costo dipende dal numero Q di dati. Per $Q = 2^n$, $Q \log_2 Q = n2^n$.

CAPITOLO 09

La ricerca quantistica del periodo

Ampiezze periodiche e interferenza



L’algoritmo di Shor

La periodicità negli esponenti

Nel problema di Simon due ingressi producono lo stesso risultato quando differiscono per una maschera binaria, applicata mediante XOR. Le potenze modulari seguono invece l'addizione ordinaria: se il periodo è r, gli esponenti x, $x + r$ e $x + 2r$ danno lo stesso resto.

Il procedimento quantistico conserva l'idea già incontrata con Simon. Il calcolo della funzione associa gli ingressi alle rispettive uscite, mentre una trasformazione successiva permette alle ampiezze di interferire. Poiché è cambiata l'operazione che descrive la ripetizione, occorre però una trasformata diversa.

La trasformata discreta di Fourier studiata nel capitolo precedente fornisce proprio la descrizione adatta alle traslazioni intere. Esaminiamo il suo effetto sui registri prima di costruirne il circuito.

Due nozioni di periodicità

Simon

$$f(x \oplus s) = f(x)$$

Potenze modulari

$$f(x + r) = f(x)$$

La trasformata deve rispettare l'operazione che definisce il periodo.

Richiami $x \oplus s$ indica lo XOR bit a bit. $x + r$ indica una somma intera con gli eventuali riporti. Per $f(x) = c^x \bmod N$, il periodo minimo soddisfa $c^r \equiv 1 \pmod N$.

Un esempio con quattro resti

Per osservare il meccanismo in pochi passaggi usiamo provvisoriamente $f(x) = 2^x \bmod 15$. Le prime potenze danno i resti $1, 2, 4, 8$, poi $2^4 = 16$ riporta al resto 1. Da quel momento la sequenza ricomincia, perché ogni nuovo termine si ottiene moltiplicando il precedente per 2 e riducendo modulo 15.

Il periodo vale dunque $r = 4$. Un registro di cinque qubit rappresenta i $Q = 32$ esponenti da 0 a 31 e contiene otto ripetizioni complete. In questo esempio il periodo divide esattamente Q, circostanza che rende particolarmente semplici i grafici.

Useremo questi numeri per capire l'interferenza. Il caso RSA con $N = 55$ tornerà quando affronteremo i picchi che non cadono esattamente su valori interi.

La funzione $f(x) = 2^x \bmod 15$

esponente x	resto $f(x)$
0	1
1	2
2	4
3	8
4	1
5	2
6	4
7	8

$1, 2, 4, 8$ si ripetono ogni quattro esponenti.

Richiami $Q = 2^n$ è il numero di etichette rappresentabili con n qubit. Qui $n = 5$, $Q = 32$ e $r = 4$. Il piccolo esempio illustra il meccanismo, non la difficoltà dei grandi moduli.

La preparazione degli esponenti

Prepariamo il primo registro in una sovrapposizione uniforme: tutti gli esponenti hanno la stessa ampiezza. Il secondo registro parte da uno stato noto.

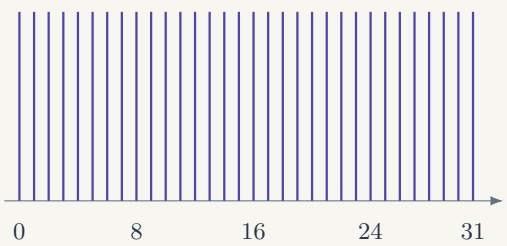
$$|\psi\rangle = \frac{1}{\sqrt{32}} \sum_{x=0}^{31} |x\rangle$$

Il fattore $1/\sqrt{32}$ assicura che le probabilità sommino a uno: ogni esponente avrebbe probabilità $1/32$ se misurassimo subito. Le etichette descrivono alternative quantistiche nello stesso registro, non valori già letti da un programma.

Il successivo calcolo reversibile agirà coerentemente su tutti i termini. Rinviando la misura potremo trasformare le ampiezze e ricavare informazioni sulla periodicità degli esponenti.

Una sovrapposizione su 32 esponenti

$$\alpha_x = 1/\sqrt{32}$$



$$p(x) = |\alpha_x|^2 = 1/32$$

$$32 \cdot (1/32) = 1$$

Richiami In $\sum_x \alpha_x |x\rangle$, α_x è un'ampiezza. La probabilità di ottenere x è $|\alpha_x|^2$ e la normalizzazione richiede $\sum_x |\alpha_x|^2 = 1$.

L’associazione fra esponenti e resti

Il calcolo reversibile della funzione conserva l’esponente nel primo registro e scrive il resto nel secondo. Agendo sulla sovrapposizione uniforme produce lo stato

$$\frac{1}{\sqrt{32}} \sum_{x=0}^{31} |x\rangle |2^x \bmod 15\rangle$$

Il termine $|5\rangle|2\rangle$, per esempio, associa all’esponente 5 il resto $2^5 \bmod 15 = 2$. L’ampiezza di questo termine è ancora $1/\sqrt{32}$. Il numero 2 scritto nel secondo registro è un’etichetta del resto e non diventa l’ampiezza del primo registro.

Occorre distinguere gli esponenti dalle ampiezze che accompagnano i termini. La QFT agirà su queste ampiezze, mentre i valori della funzione resteranno nel secondo registro.

Esponente e resto nello stesso termine

primo registro	secondo registro
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|2\rangle$
$\|2\rangle$	$\|4\rangle$
$\|3\rangle$	$\|8\rangle$
$\|4\rangle$	$\|1\rangle$
$\|5\rangle$	$\|2\rangle$

Ogni coppia ha ampiezza $1/\sqrt{32}$.

Richiami $|x\rangle|f(x)\rangle$ rappresenta una coppia di registri. I resti sono $f(x) \in \{1, 2, 4, 8\}$, mentre le ampiezze dei 32 termini sono tutte $1/\sqrt{32}$.

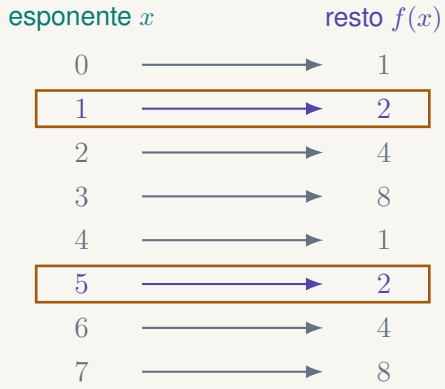
Gli esponenti associati al resto 2

Immaginiamo di misurare il secondo registro e di ottenere il resto 2. Le sole coppie compatibili con questo esito sono quelle per cui $2^x \bmod 15 = 2$. Gli esponenti possibili sono quindi $1, 5, 9, 13, 17, 21, 25, 29$.

La misura distingue il valore della funzione, ma non distingue fra gli otto esponenti che lo producono. Nel primo registro rimane perciò una sovrapposizione di questi ingressi, con ampiezze uguali dopo la normalizzazione.

Il risultato 2 compare in otto dei trentadue termini iniziali, quindi ha probabilità $8/32 = 1/4$. Avremmo potuto ottenere anche 1, 4 oppure 8. Ciascun risultato seleziona una successione di esponenti con la stessa distanza $r = 4$, ma con un diverso punto iniziale.

La funzione $f(x) = 2^x \bmod 15$



$1, 2, 4, 8$ si ripetono ogni quattro esponenti.

Richiami Fissato un resto f_0, gli esponenti compatibili sono $x = x_0 + kr$. Qui $f_0 = 2$, $x_0 = 1$ e $k = 0, \ldots, 7$. La misura del secondo registro serve a chiarire l'analisi.

Una sovrapposizione di posizioni equidistanti

Lo stato rimasto nel primo registro contiene esattamente l'informazione che cerchiamo: la distanza fra due esponenti consecutivi è il periodo. Possiamo scriverlo in forma compatta come

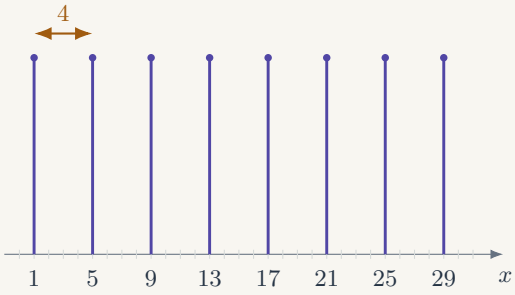
$$|\psi_1\rangle = \frac{1}{\sqrt{8}} \sum_{k=0}^{7} |1 + 4k\rangle$$

Il grafico delle ampiezze ha l'aspetto di un pettine. Ogni stelo indica un'ampiezza $1/\sqrt{8}$, mentre le altre posizioni hanno ampiezza nulla. Ciascuno degli otto esponenti ha dunque probabilità $1/8$.

Il pedice 1 ricorda il punto iniziale $x_0 = 1$. Un altro risultato nel secondo registro sposterebbe il pettine, lasciando invariata la distanza che dobbiamo estrarre.

Ampiezze del primo registro

Otto ampiezze uguali a $1/\sqrt{8}$



$$x = 1 + 4k, \quad k = 0, \ldots, 7$$

La distanza fra gli steli è $r = 4$.

Richiami Il pettine è il grafico delle ampiezze del registro degli esponenti. Non è il grafico dei resti $2^x \bmod 15$. Qui $8 \cdot |1/\sqrt{8}|^2 = 1$.

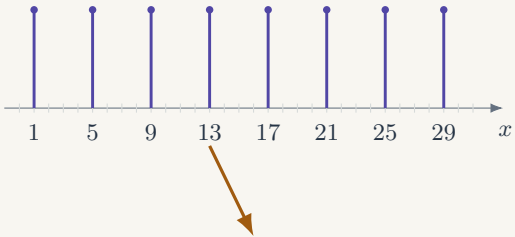
Il limite di una misura immediata

Una misura del primo registro potrebbe restituire 13, con probabilità $1/8$. Dopo questa lettura conosceremmo un esponente compatibile con il resto 2, ma non l'elenco delle altre posizioni presenti nella sovrapposizione.

La distanza 4 risulta evidente nel disegno perché il disegno mostra l'intero stato. Un dispositivo di misura restituisce invece uno dei suoi possibili esiti. Non possiamo trattare quel disegno come una tabella che il computer possa leggere riga per riga.

Ripetere tutta la preparazione può inoltre produrre un altro resto nel secondo registro e quindi un pettine traslato. Occorre prima trasformare lo stato in modo che le probabilità della lettura finale dipendano dal periodo in una forma utilizzabile. Questo è il compito della QFT.

Una lettura restituisce un solo esponente



Un esito non elenca le posizioni del pettine.

Richiami Una misura nella base computazionale restituisce un'etichetta x con probabilità $|\alpha_x|^2$. Il periodo è una proprietà della disposizione delle ampiezze, non del singolo esito.

La trasformata di Fourier delle ampiezze

La trasformata quantistica di Fourier realizza sullo stato la trasformazione discreta già studiata. Adottiamo la convenzione con segno positivo nell'esponenziale:

$$\mathrm{QFT}_Q|x\rangle = \frac{1}{\sqrt{Q}} \sum_{y=0}^{Q-1} e^{2\pi i x y/Q} |y\rangle$$

La formula specifica l'effetto su un ingresso di base. Per linearità determina anche l'effetto su qualsiasi sovrapposizione: ogni ampiezza iniziale contribuisce alle ampiezze finali con una fase che dipende da x e da y.

I coefficienti di Fourier diventano le nuove ampiezze. La misura restituisce un solo indice y, con probabilità pari al modulo quadro del suo coefficiente. La lista completa dei coefficienti rimane inaccessibile a questa lettura.

La trasformata opera sulle ampiezze

$$|\psi\rangle = \Sigma_x \, \alpha_x |x\rangle$$

$$\downarrow$$

$$\mathrm{QFT}$$

$$\downarrow$$

$$|\widetilde{\psi}\rangle = \Sigma_y \, \beta_y |y\rangle$$

$$\beta_y = \frac{1}{\sqrt{Q}} \Sigma_x \, \alpha_x e^{2\pi i x y/Q}$$

La misura restituisce y con probabilità $|\beta_y|^2$.

Richiami $i^2 = -1$ e $e^{i\theta} = \cos\theta + i \sin\theta$. x etichetta gli ingressi, y gli esiti dopo la trasformata. Il fattore $1/\sqrt{Q}$ rende la trasformazione unitaria.

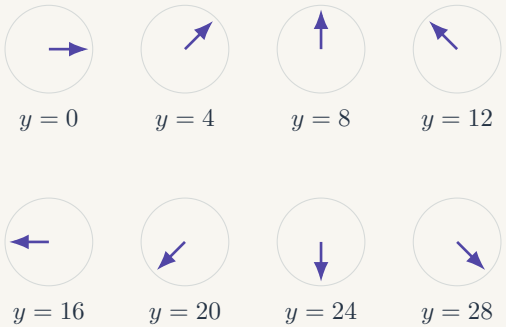
Le fasi generate da un solo esponente

Consideriamo per un momento il solo ingresso $|1\rangle$. Per $Q = 32$, la sua trasformata assegna a ogni uscita y un'ampiezza di modulo $1/\sqrt{32}$ e di fase $2\pi y/32$.

Quando y aumenta, la freccia che rappresenta il coefficiente ruota nel piano complesso. Per $y = 0$ punta verso destra, per $y = 8$ verso l'alto, per $y = 16$ verso sinistra e per $y = 24$ verso il basso. Il grafico include anche le direzioni intermedie.

Il modulo è identico per tutte le uscite, quindi la trasformata di un singolo esponente non produce picchi di probabilità. I picchi compaiono quando più esponenti contribuiscono alla stessa uscita: allora le loro frecce possono sommarsi oppure cancellarsi. È la situazione del nostro pettine periodico.

Le fasi prodotte dall'ingresso $|1\rangle$



$$\arg \beta_y = 2\pi y/32$$
Campioni: $y = 0, 4, 8, \ldots, 28.$

Richiami Per l'ingresso $|1\rangle$, $\beta_y = e^{2\pi i y/32}/\sqrt{32}$ e $|\beta_y|^2 = 1/32$. Le frecce mostrano la fase, mentre la loro lunghezza è uguale per tutte le uscite.

Il contributo degli otto esponenti

Applichiamo ora la QFT alla sovrapposizione degli otto ingressi $1 + 4k$. Per ogni uscita y dobbiamo sommare otto contributi. Separando il termine che dipende dal punto iniziale otteniamo

$$\beta_y = \frac{e^{2\pi i y/32}}{16} \sum_{k=0}^{7} e^{2\pi i (4k) y/32}$$

Il denominatore 16 deriva da $\sqrt{8}\sqrt{32}$. Nella somma, due contributi consecutivi differiscono per una rotazione di angolo $2\pi\, 4y/32$. Quando questa rotazione è un giro intero, tutte le frecce sono concordi. Per altre uscite, le direzioni distribuiscono i contributi attorno al cerchio.

Il fattore esterno ha modulo uno: la probabilità dipende dalla lunghezza della somma delle otto frecce, indipendentemente da questa fase iniziale.

La trasformata opera sulle ampiezze

$$|\psi\rangle = \Sigma_x\, \alpha_x |x\rangle$$

$$\downarrow$$

$$\text{QFT}$$

$$\downarrow$$

$$|\widetilde{\psi}\rangle = \Sigma_y\, \beta_y |y\rangle$$

$$\beta_y = \frac{1}{\sqrt{Q}} \Sigma_x\, \alpha_x e^{2\pi i x y/Q}$$

La misura restituisce y con probabilità $|\beta_y|^2$.

Richiami Per il pettine $x_0 + kr$, la differenza di fase fra contributi adiacenti è $\Delta\theta = 2\pi r y/Q$. La probabilità finale è $p(y) = |\beta_y|^2$.

Una frequenza compatibile con il periodo

Per l'uscita $y = 8$, la rotazione fra due contributi consecutivi vale $2\pi \cdot 4 \cdot 8/32 = 2\pi$. Un giro completo riporta ogni freccia nella stessa direzione, perciò gli otto contributi si sommano senza cancellazioni.

$$|\beta_8| = \frac{8}{16} = \frac{1}{2}, \qquad p(8) = \frac{1}{4}$$

Nel diagramma abbiamo tolto la fase esterna comune e rappresentato le otto frecce nella direzione reale positiva. Ripristinare quella fase ruota il risultato, senza modificarne la lunghezza o la probabilità.

La stessa concordanza si verifica per $y = 0$, 16 e 24, perché anche in questi casi la rotazione fra contributi è un multiplo di un giro. Le uscite favorite sono dunque separate da $Q/r = 8$.

Contributi alla frequenza $y = 8$



$1 + 1 + \cdots + 1 = 8$

otto frecce coincidenti

$|\beta_8| = 8/16 = 1/2$

$$p(8) = |\beta_8|^2 = 1/4$$

Abbiamo separato la fase comune $e^{2\pi i x_0 y/32}$.

Richiami Le fasi sono concordi quando ry/Q è un intero. Nel caso $Q = 32$, $r = 4$, ciò avviene per $y = 0, 8, 16, 24$. Una fase di modulo uno non cambia $|\beta_y|^2$.

Una frequenza cancellata dall'interferenza

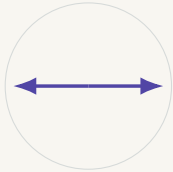
Consideriamo invece l'uscita $y = 4$. La rotazione fra due esponenti consecutivi del pettine è ora $2\pi \cdot 4 \cdot 4/32 = \pi$: ogni freccia punta nella direzione opposta alla precedente.

$$1 - 1 + 1 - 1 + 1 - 1 + 1 - 1 = 0$$

La somma delle ampiezze è nulla e la misura non può restituire questa uscita. Le probabilità non si sommano prima della trasformata: sono le ampiezze complesse a combinarsi, e solo dopo si calcola il modulo quadro.

Per gli altri valori che non sono multipli di 8, le frecce formano poligoni chiusi e la cancellazione è completa. La disposizione periodica degli esponenti determina così le frequenze che sopravvivono all'interferenza.

Contributi alla frequenza $y = 4$



$1 - 1 + 1 - 1 + \cdots = 0$

coppie opposte

$$\beta_4 = 0$$

$$p(4) = 0$$

Abbiamo separato la fase comune $e^{2\pi i x_0 y/32}$.

Richiami Il numero complesso $e^{i\pi} = -1$ rappresenta una rotazione di mezzo giro. Se la somma delle ampiezze per un esito è zero, anche la probabilità di quell'esito è zero.

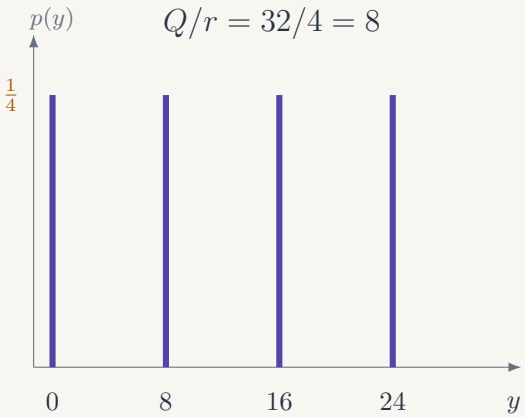
Le quattro uscite possibili

Riunendo i due tipi di comportamento otteniamo una distribuzione molto semplice. Le sole uscite possibili sono 0, 8, 16 e 24, tutte con probabilità $1/4$. La normalizzazione si controlla immediatamente sommando le quattro probabilità.

Il pettine iniziale aveva otto posizioni occupate, separate da $r = 4$. Il grafico finale ha quattro picchi, separati da $Q/r = 8$. La trasformata ha convertito la distanza fra gli esponenti in una spaziatura fra le frequenze.

Una singola esecuzione non mostra l'intero grafico: restituisce una delle quattro ascisse. Sappiamo però che ciascuna ascissa è un multiplo di Q/r. Questa relazione aritmetica è ciò che useremo per ricostruire il periodo a partire dal risultato della misura.

Le probabilità dopo la QFT



Quattro esiti equiprobabili; la somma delle probabilità vale 1.

Richiami Quando r divide Q, i picchi sono esattamente in $y = jQ/r$, con $j = 0, \ldots, r-1$. Il grafico rappresenta una distribuzione di probabilità, non l'output completo di una singola esecuzione.

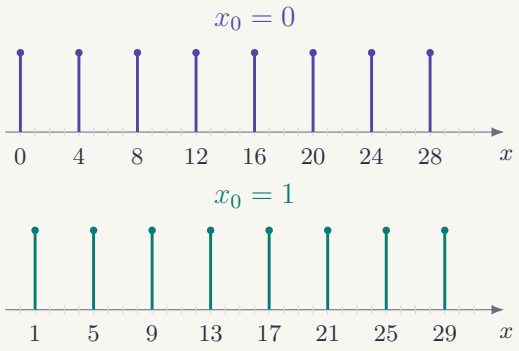
L’indipendenza dal punto iniziale

Il risultato della misura del secondo registro determina il punto iniziale x_0, che può valere 0, 1, 2 oppure 3. Con $x_0 = 0$ gli esponenti sono $0, 4, 8, \ldots$; con $x_0 = 1$ diventano $1, 5, 9, \ldots$. In entrambi i casi la distanza resta 4.

Nella trasformata, questa traslazione compare nel fattore $e^{2\pi i x_0 y/Q}$. Il fattore dipende dall’uscita y e può quindi cambiare le fasi relative dello stato finale. Poiché il suo modulo vale uno, scompare però nel calcolo di ciascuna probabilità.

Nel nostro esempio tutti e quattro i pettini producono così gli stessi picchi. Possiamo raccogliere informazioni sul periodo anche se la preparazione seleziona ogni volta un diverso punto iniziale.

Pettini traslati di una posizione



$p(y) = 1/4$ per $y = 0, 8, 16, 24$

Caso esatto: r divide Q.

Richiami $|e^{i\theta} z|^2 = |z|^2$. Il fattore di traslazione dipende da y: non è una fase globale dell’intero stato. Qui la distribuzione è esattamente indipendente da x_0 perché $r \mid Q$.

Il secondo registro può restare non misurato

Abbiamo introdotto la misura del secondo registro per isolare un pettine alla volta. L'algoritmo può però applicare la QFT al primo registro senza leggere il secondo.

Il secondo registro mantiene distinguibili le coppie associate a resti diversi. Osservando soltanto il primo, le probabilità di queste alternative si combinano secondo i loro pesi. Qui ogni resto ha peso $1/4$ e ogni pettine produce la stessa distribuzione finale.

La misura intermedia, eseguita e poi ignorata oppure omessa, conduce quindi alle stesse probabilità per y. La possibilità di ometterla vale anche nel caso generale. Il pettine aiuta a comprendere l'analisi, senza imporre un'operazione aggiuntiva al circuito.

I quattro resti possibili

$$f_0 = 1 \longrightarrow x = 0,\ 4,\ 8, \ldots$$

$$f_0 = 2 \longrightarrow x = 1,\ 5,\ 9, \ldots$$

$$f_0 = 4 \longrightarrow x = 2,\ 6,\ 10, \ldots$$

$$f_0 = 8 \longrightarrow x = 3,\ 7,\ 11, \ldots$$

Ogni classe produce
gli stessi quattro picchi.

Richiami La QFT agisce sul registro degli esponenti. Il secondo registro conserva il valore $f(x)$. Misurare quel registro e ignorarne l'esito non cambia le statistiche di una successiva misura sul primo.

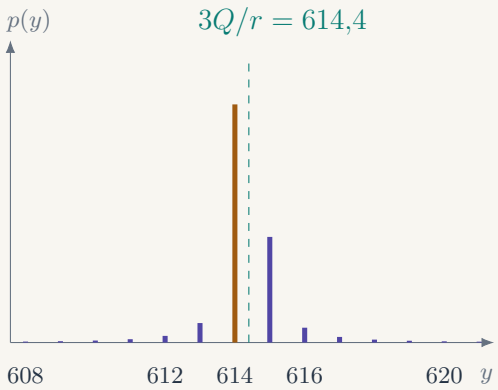
I picchi quando il periodo non divide il registro

Torniamo al cifrato 13 modulo 55, il cui periodo è 20. Un registro con $Q = 4096$ posizioni contiene molti periodi, ma $4096/20 = 204{,}8$ non è un intero. I punti in cui le fasi sarebbero perfettamente concordi possono quindi trovarsi fra due etichette misurabili.

I picchi rimangono concentrati vicino ai multipli di Q/r. Per esempio, il terzo si trova vicino a $3 \cdot 4096/20 = 614{,}4$, mentre una misura può restituire soltanto un intero, come 614 oppure 615. Il grafico mostra il dettaglio della distribuzione per un pettine con $x_0 = 1$.

Il procedimento non richiede che il periodo sia una potenza di due. Richiede invece abbastanza precisione per ricostruire una frazione dal valore misurato. Il prossimo capitolo sviluppa questo passaggio e lo collega alla decifrazione.

Il caso RSA: $Q = 4096$, $r = 20$



Un picco può cadere fra due interi.

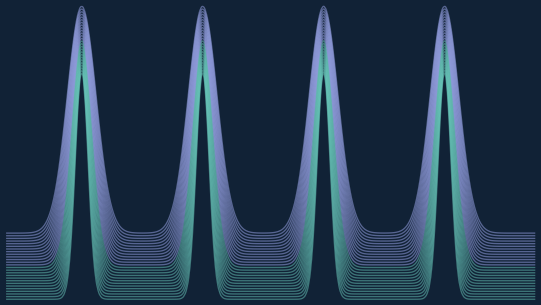
Dettaglio delle probabilità per $x_0 = 1$.

Richiami Nel caso generale i picchi sono vicini a $y \simeq jQ/r$. Dividendo per il valore noto Q otteniamo $y/Q \simeq j/r$. La misura fornisce y, mentre j e r restano da ricostruire.

CAPITOLO 10

Dalla misura al messaggio

Approssimazioni razionali e decifrazione



L’algoritmo di Shor

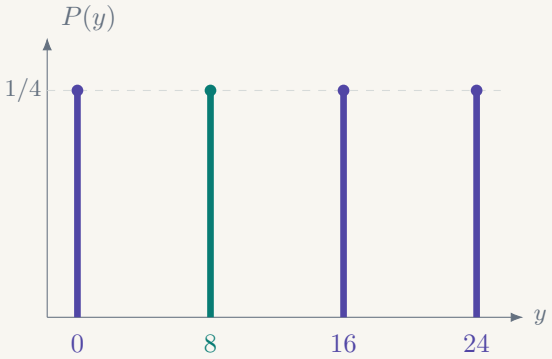
Il significato del numero misurato

Nel caso esatto studiato finora, il registro contiene $Q = 32$ posizioni e il pettine ha periodo $r = 4$. La trasformata concentra le probabilità in $y = 0, 8, 16, 24$. Al termine di un'esecuzione il dispositivo restituisce uno solo di questi interi, scritto sui cinque qubit del registro.

Supponiamo di leggere $y = 8$. Dividendo per la dimensione del registro otteniamo $8/32 = 1/4$. Il denominatore coincide con il periodo, poiché in questo caso abbiamo osservato il primo picco dopo lo zero.

Il passaggio generale è $y/Q = j/r$: l'indice j del picco rimane sconosciuto. Dobbiamo quindi ricavare il denominatore della frazione, tenendo conto delle possibili semplificazioni. Il valore misurato y, da solo, non è ancora il periodo.

Quattro esiti possibili, un solo periodo



Esito $y = 8$: $\quad y/Q = 8/32 = 1/4$

Il denominatore restituisce $r = 4$.

Richiami $Q = 2^n$ è il numero di stati del registro. Se r divide Q, gli esiti ammessi sono $y = jQ/r$, con $j = 0, \ldots, r-1$.

Un denominatore ridotto può nascondere il periodo

Con lo stesso periodo $r = 4$, la misura può restituire $y = 16$. Il rapporto $16/32$ vale $1/2$, sebbene il picco corrisponda a $j/r = 2/4$. La semplificazione ha cancellato il fattore comune 2 e il denominatore rimasto è soltanto un divisore del periodo.

Gli esiti 8 e 24 restituiscono invece $1/4$ e $3/4$, entrambe già ridotte ai minimi termini. Quando numeratore e denominatore sono coprimi, la frazione conserva il periodo intero.

L'esito zero non fornisce un denominatore utile. Una nuova esecuzione può produrre un'altra frazione e completare l'informazione precedente. La necessità di ripetere il procedimento nasce già in questo esempio perfetto, anche in assenza di errori del dispositivo.

La riduzione ai minimi termini

$j = 1$	$1/4$	denominatore 4
$j = 2$	$2/4 = 1/2$	denominatore 2
$j = 3$	$3/4$	denominatore 4
$j = 0$	$0/4 = 0$	nessuna informazione

Richiami Una frazione è ai minimi termini quando numeratore e denominatore hanno MCD uguale a 1. Riducendo j/r, il denominatore diventa $r/\operatorname{MCD}(j, r)$.

La dimensione dei registri nell'esempio RSA

Riprendiamo il cifrato $c = 13$ e il modulo $N = 55$. La funzione è $f(x) = 13^x \bmod 55$, il cui periodo, ancora ignoto all'attaccante, è 20. I suoi valori occupano soltanto sei bit, perché tutti i resti sono minori di $55 < 2^6$.

Il registro degli esponenti deve essere più ampio. Scegliamo dodici qubit, dunque $Q = 2^{12} = 4096$ posizioni. La disuguaglianza $4096 > 55^2$ garantirà la precisione necessaria alla ricostruzione della frazione j/r.

Il periodo 20 non divide 4096. Le posizioni del pettine occupano quindi una finestra che si interrompe durante l'ultima ripetizione. È la situazione generale da affrontare: il caso precedente, con $r = 4$ e $Q = 32$, serviva a osservare il meccanismo senza questa complicazione.

Due registri con compiti distinti

Esponenti x



12 qubit: $Q = 2^{12} = 4096$

Resti $f(x)$



6 qubit: $0 \le f(x) < 55 < 64$

$55^2 = 3025 < 4096$

Richiami Il registro dei valori rappresenta i resti modulo N. Il registro degli esponenti ha $Q = 2^n$ posizioni, con $Q > N^2$ nella scelta qui adottata.

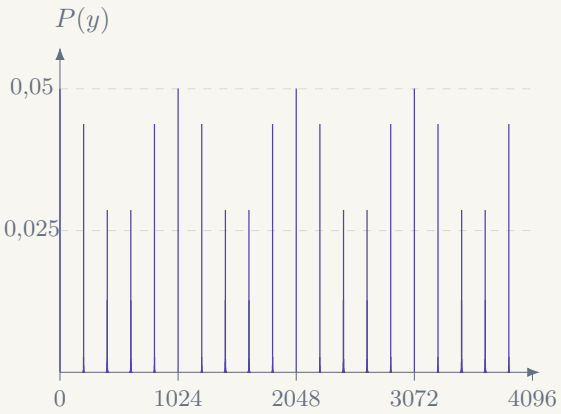
Picchi vicini ai multipli di una frequenza

Quando r non divide Q, i contributi della trasformata non si cancellano esattamente in tutte le posizioni intermedie. Rimangono tuttavia forti concentrazioni di probabilità vicino ai multipli di Q/r. Nel nostro esempio la loro distanza è $4096/20 = 204{,}8$.

Il primo centro è in 0, seguito da $204{,}8$ e $409{,}6$, poi da $614{,}4$. Una misura può restituire soltanto un intero. Il grafico mostra la probabilità calcolata per il pettine che comincia in $x_0 = 1$ e contiene 205 termini.

Le probabilità si distribuiscono fra gli interi vicini a ciascun centro. La ricostruzione dovrà perciò tollerare un piccolo errore. Il valore di r riportato nel disegno serve a interpretare l'esempio e rimane ciò che il procedimento deve ricavare.

Probabilità dopo la QFT, $Q = 4096$



Centri dei picchi: $y \simeq j\,204{,}8$

Condizionamento $x_0 = 1$;
205 termini nel pettine.

Richiami Con L termini nel pettine, $P(y) = \frac{1}{QL}\left|\sum_{k=0}^{L-1} e^{2\pi i k r y/Q}\right|^2$. Qui $Q = 4096$, $r = 20$, $L = 205$.

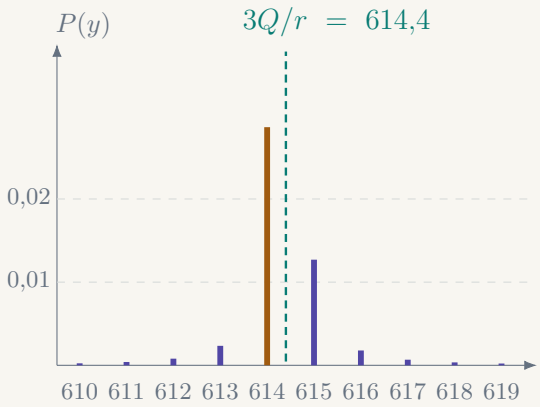
La misura 614 e una frazione vicina

Consideriamo un'esecuzione che restituisca $y = 614$. Il picco vicino ha centro $3Q/r = 614{,}4$, dunque l'esito dista appena $0{,}4$ da quel valore. L'attaccante conosce il numero misurato e la dimensione del registro, perciò può formare il rapporto $614/4096$.

Questa frazione vale $0{,}14990234375$, molto vicino a $0{,}15 = 3/20$. La differenza è circa $0{,}00009766$. Riconoscendo la frazione $3/20$, otteniamo il candidato 20 per il periodo.

La vicinanza visibile dei decimali rende plausibile il risultato, ma non costituisce ancora un metodo di calcolo. Occorre spiegare quanta precisione serva e come riconoscere la frazione senza provare tutti i denominatori possibili.

Un picco fra due valori interi



$614/4096 = 0{,}14990234375$

$3/20 = 0{,}15$

Richiami Il rapporto osservabile è y/Q. L'indice del picco j e il periodo r sono sconosciuti. Un esito favorevole approssima j/r.

La precisione necessaria alla ricostruzione

Se l'intero misurato y dista al più $1/2$ dal centro jQ/r, dividendo per Q otteniamo un errore non superiore a $1/(2Q)$. La frazione cercata appartiene quindi a un intervallo di ampiezza totale $1/Q$.

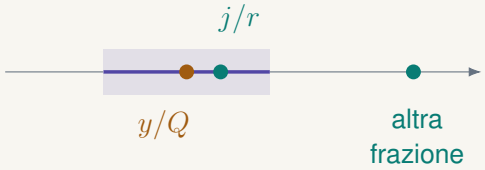
D'altra parte, due frazioni distinte a/b e u/v, con denominatori minori di N, distano almeno $1/(bv) > 1/N^2$. Infatti il numeratore della differenza, $av - bu$, è un intero non nullo e ha valore assoluto almeno 1.

La scelta $Q > N^2$ rende l'intervallo compatibile con la misura più stretto della separazione minima. Vi può entrare una sola frazione distinta con denominatore minore di N. Questo argomento vale per un esito favorevole, non per ogni risultato della misura.

Una misura precisa distingue due frazioni

$$\left| \frac{y}{Q} - \frac{j}{r} \right| \leq \frac{1}{2Q}$$

Intervallo compatibile: ampiezza totale $1/Q$



Denominatori $< N$: distanza $> 1/N^2$

$Q > N^2$ rende l'intervallo più stretto.

Richiami Per le potenze di un numero coprimo con N, il periodo soddisfa $r < N$. Qui $N^2 = 3025$ e $Q = 4096$. Il disegno illustra le distanze, senza scala numerica.

Le frazioni continue attraverso le divisioni

Per riconoscere la frazione utile impieghiamo le frazioni continue. Il procedimento riprende le divisioni dell'algoritmo di Euclide, che abbiamo già usato per calcolare il massimo comun divisore. Prima riduciamo $614/4096$ a $307/2048$.

Dividiamo 2048 per 307: il quoziente è 6 e il resto 206. Poi dividiamo 307 per 206, ottenendo quoziente 1 e resto 101. Continuando, i quozienti successivi sono $2, 25, 4$.

Questi numeri descrivono la frazione come una successione di reciproci: $[0; 6, 1, 2, 25, 4]$. Lo zero iniziale compare perché $307/2048 < 1$. Interrompere la successione dopo pochi quozienti produce frazioni con denominatori piccoli, che possono già approssimare accuratamente la misura.

Gli stessi resti dell'algoritmo di Euclide

$$2048 = 6 \cdot 307 + 206$$

$$307 = 1 \cdot 206 + 101$$

$$206 = 2 \cdot 101 + 4$$

$$101 = 25 \cdot 4 + 1$$

$$4 = 4 \cdot 1$$

$$\frac{307}{2048} = [0; 6, 1, 2, 25, 4]$$

Richiami La notazione $[a_0; a_1, a_2, \ldots]$ significa $a_0 + 1/(a_1 + 1/(a_2 + \cdots))$. I quozienti si ottengono mediante divisioni con resto.

Il denominatore 20 nei convergenti

Le frazioni ottenute interrompendo una frazione continua si chiamano convergenti. Dal primo quoziente ricaviamo $[0;6] = 1/6$. Conservando anche il secondo troviamo $[0;6,1] = 1/7$. Con il terzo compare $[0;6,1,2] = 3/20$.

Il terzo valore approssima il rapporto misurato con errore inferiore a $1/(2Q)$. I primi due sono troppo lontani. Il denominatore 20 è inoltre minore di $N = 55$, come deve essere il periodo della funzione.

Un risultato delle frazioni continue garantisce che una frazione ridotta j/r, approssimata con errore minore di $1/(2r^2)$, compare fra i convergenti. La precisione scelta per il registro soddisfa questa condizione negli esiti favorevoli. Il passo seguente consiste nel controllare il candidato ottenuto.

Approssimazioni via via più accurate

$[0;6]$	$1/6$	$0{,}166667$
$[0;6,1]$	$1/7$	$0{,}142857$
$[0;6,1,2]$	$3/20$	$0{,}150000$

Valore misurato: $0{,}14990234375$

$$\frac{1}{6 + \frac{1}{1+\frac{1}{2}}} = \frac{3}{20}$$

Richiami Un convergente usa soltanto i primi quozienti. Il criterio di ricostruzione riguarda la frazione j/r ridotta ai minimi termini, il cui denominatore può dividere r.

Il controllo aritmetico del candidato

Il candidato $R = 20$ supera il controllo $13^{20} \bmod 55 = 1$. Questo certifica che dopo venti passi si ritorna a 1, ma il periodo minimo potrebbe, in linea di principio, essere un divisore di 20.

Nel piccolo esempio possiamo controllare anche la minimalità. I divisori propri di 20 sono $1, 2, 4, 5, 10$. Il calcolo $13^{10} \bmod 55 = 34$ esclude tutti quelli che dividono 10. Il calcolo $13^4 \bmod 55 = 16$ esclude il divisore 4. Rimane soltanto $r = 20$.

Per decifrare può bastare anche un multiplo verificato dell'ordine, purché l'esponente pubblico ammetta un inverso modulo quel multiplo. La prova di minimalità appena svolta chiarisce la definizione di periodo, senza imporre una nuova fattorizzazione alla procedura.

Il controllo del candidato 20

$$13^{20} \equiv 1 \pmod{55}$$

Il periodo divide 20.

$$13^{10} \equiv 34 \neq 1 \pmod{55}$$

Esclusi $1, 2, 5, 10$.

$$13^4 \equiv 16 \neq 1 \pmod{55}$$

Esclusi anche 4 e i suoi divisori.

Il primo ritorno avviene a $r = 20$.

Richiami Se $c^R \equiv 1 \pmod{N}$, l'ordine r divide R. L'ordine è il minimo esponente positivo che produce 1. Le potenze si verificano con quadrati successivi.

Informazioni complementari da misure diverse

Un'esecuzione potrebbe restituire $y = 1024$, da cui otteniamo $1024/4096 = 1/4$. La frazione ideale era $5/20$, ma il fattore comune 5 è scomparso. Un'altra esecuzione potrebbe dare $y = 819$, vicino al picco $4Q/20 = 819{,}2$. Le frazioni continue riconoscono allora $1/5$.

I denominatori 4 e 5, presi separatamente, non sono periodi: $13^4 \bmod 55 = 16$ e $13^5 \bmod 55 = 43$. Il loro minimo comune multiplo è invece 20, che supera il controllo di ritorno a 1.

Le ripetizioni possono dunque recuperare fattori cancellati da una singola riduzione. Il minimo comune multiplo si calcola efficientemente tramite il MCD. Se i controlli falliscono, si raccolgono nuove misure senza enumerare tutti i possibili periodi.

Due esecuzioni possono completarsi

Prima misura	Seconda misura
$y = 1024$	$y = 819$
$1024/4096 = 1/4$	$819/4096 \simeq 1/5$
$5/20 = 1/4$	$4/20 = 1/5$

$$\operatorname{mcm}(4, 5) = 20$$

Controllo finale: $13^{20} \bmod 55 = 1$

Richiami $\operatorname{mcm}(u, v) = uv/\operatorname{MCD}(u, v)$. Quando le frazioni recuperate sono corrette, i loro denominatori dividono il periodo e il loro mcm lo divide a sua volta.

Verifica degli esiti e ripetizioni

La misura può cadere lontano da un picco utile e suggerire un denominatore che non divide il periodo. I calcoli successivi includono perciò un controllo della potenza modulare.

Indichiamo con R il candidato ricavato da una o più esecuzioni. Se $c^R \equiv 1 \pmod{N}$ e $\mathrm{MCD}(e, R) = 1$, possiamo trovare $d_c = e^{-1} \pmod{R}$. Poiché il vero ordine divide R, la stessa dimostrazione del capitolo 6 garantisce la decifrazione.

Una prova fallita richiede altre misure. Una prova riuscita fornisce una conferma aritmetica con calcoli classici efficienti. La casualità determina l'informazione raccolta in una singola esecuzione, mentre le verifiche permettono di riconoscere un candidato utilizzabile.

Un candidato deve superare i controlli

$$R \text{ ricavato dalle misure}$$
$$\downarrow$$
$$13^R \bmod 55 = 1$$
$$\downarrow$$
$$\mathrm{MCD}(3, R) = 1$$
$$\downarrow$$
$$d_c = 3^{-1} \pmod{R}$$

Controlli falliti: una nuova esecuzione.

Richiami R è un candidato, anche non minimo. Le condizioni $c^R \equiv 1 \pmod{N}$ e $\mathrm{MCD}(e, R) = 1$ bastano a costruire un esponente che decifri quel cifrato.

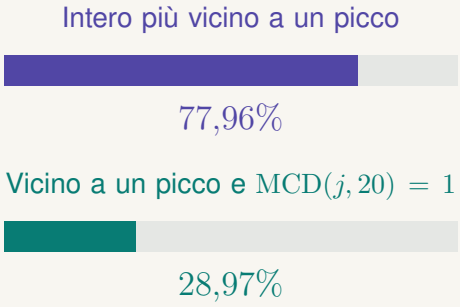
La probabilità di una misura utile

Nel pettine dell'esempio, la somma delle probabilità degli interi più vicini ai venti picchi vale circa $77{,}96\%$. Soltanto una parte di questi esiti conserva il denominatore intero: quelli con $\mathrm{MCD}(j, 20) = 1$ hanno probabilità complessiva circa $28{,}97\%$. Gli altri possono fornire divisori utili da combinare.

Nel caso generale l'analisi garantisce una quota costante di misure vicine ai picchi. Occorre poi considerare le semplificazioni delle frazioni e le ripetizioni, senza confondere queste probabilità distinte.

L'analisi di Shor mostra che anche tali passaggi mantengono il costo complessivo polinomiale nel numero di bit dell'ingresso. Il vantaggio quantistico sopravvive quindi alla ricostruzione classica: la procedura non richiede un numero esponenziale di tentativi.

Probabilità calcolate per $Q = 4096$, $r = 20$



Probabilità condizionate a $x_0 = 1$.

Richiami Le percentuali nel disegno riguardano il caso numerico specifico. La vicinanza a un picco permette di recuperare una frazione, il cui denominatore può essere soltanto un divisore del periodo.

L’esponente di decifrazione dal periodo

Ora conosciamo il periodo $r = 20$ del cifrato $c = 13$. L’esponente pubblico è $e = 3$, dunque cerchiamo un numero d_c per cui $3d_c$ lasci resto 1 nella divisione per 20. È precisamente il problema dell’inverso modulare già incontrato nella costruzione di RSA.

L’algoritmo di Euclide dà $20 = 6 \cdot 3 + 2$ e $3 = 2 + 1$. Risalendo dalle divisioni, scriviamo $1 = 7 \cdot 3 - 20$. Il coefficiente 7 fornisce quindi l’inverso cercato: $d_c = 7$.

Non abbiamo usato i fattori segreti del modulo per compiere questo passaggio. Il periodo trovato mediante il calcolo quantistico ha fornito il modulo rispetto al quale invertire l’esponente pubblico. La decifrazione finale richiede soltanto una potenza modulare.

L’inverso di 3 modulo 20

$$20 = 6 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$1 = 3 - (20 - 6 \cdot 3)$$

$$1 = 7 \cdot 3 - 20$$

$$d_c = 7$$

Richiami d_c soddisfa $ed_c \equiv 1 \pmod{r}$ e consente di decifrare il cifrato considerato. Non è necessariamente la chiave privata universale d.

Il recupero del messaggio 7

Calcoliamo infine $c^{d_c} \bmod N = 13^7 \bmod 55$. La scomposizione $7 = 4 + 2 + 1$ permette di riutilizzare le potenze ottenute per quadrati successivi. Abbiamo $13^2 \equiv 4$ e $13^4 \equiv 16$ modulo 55.

Il prodotto richiesto è perciò congruo a $16 \cdot 4 \cdot 13 = 832$. Dividendo 832 per 55 otteniamo quoziente 15 e resto 7. Quest'ultimo è il messaggio recuperato. Possiamo controllarlo pubblicamente: $7^3 = 343 = 6 \cdot 55 + 13$, quindi la sua cifratura restituisce proprio il cifrato intercettato.

L'attacco ha usato i soli dati pubblici $N = 55$, $e = 3$, $c = 13$, insieme all'informazione sul periodo. Il calcolo quantistico ha reso accessibile questa informazione, mentre inversione, esponenziazione e controllo finale sono rimasti operazioni classiche.

La decifrazione con tre potenze

$$13^2 \equiv 4 \pmod{55}$$

$$13^4 \equiv 4^2 = 16 \pmod{55}$$

$$13^7 = 13^4 \cdot 13^2 \cdot 13$$

$$16 \cdot 4 \cdot 13 = 832$$

$$832 = 15 \cdot 55 + \boxed{7}$$

Richiami La cifratura è $c = m^e \bmod N$. Per questo cifrato, il periodo $r = 20$ dà $d_c = 7$ e la decifrazione è $m = c^{d_c} \bmod N$.

Il procedimento completo prima del circuito

Il cifrato determina una funzione periodica facile da valutare. Il registro quantistico associa agli esponenti i valori della funzione. Da queste correlazioni emerge il pettine periodico, sul quale la QFT produce picchi di probabilità legati al periodo.

La misura restituisce un intero. Le frazioni continue e i controlli modulari permettono di ricavarne un ordine utile, eventualmente combinando più esecuzioni. Da quell'ordine si calcola un esponente di decifrazione e si recupera il messaggio.

Rimane da realizzare le trasformazioni impiegate. Nel capitolo seguente costruiremo il circuito, riconoscendo in ciascun gruppo di porte un'operazione già compresa. Il caso numerico a destra riassume i passaggi senza richiedere la fattorizzazione di 55.

Il messaggio recuperato dai dati pubblici

$$N = 55,\ e = 3,\ c = 13$$

$$\downarrow$$

Misura quantistica: $y = 614$

$$\downarrow$$

$$614/4096 \simeq 3/20,\ r = 20$$

$$\downarrow$$

$$3d_c \equiv 1 \pmod{20},\ d_c = 7$$

$$\downarrow$$

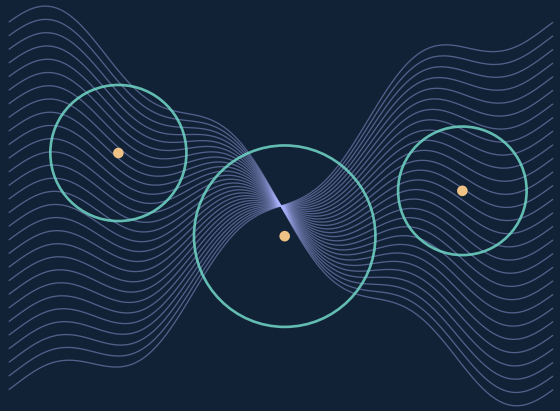
$$c^{d_c} \bmod N = 7$$

Richiami Parte quantistica: preparazione, calcolo reversibile, QFT e misura. Parte classica: frazioni continue, verifiche modulari, inverso dell'esponente e decifrazione.

CAPITOLO 11

La realizzazione del circuito

Porte, aritmetica reversibile e misura



L'algoritmo di Shor

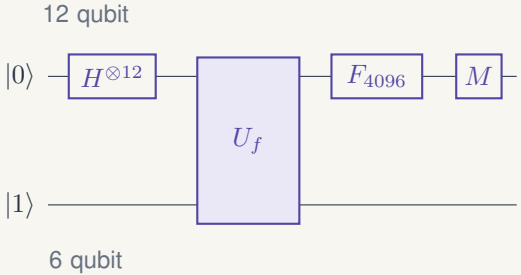
I registri e le operazioni del circuito

Il procedimento appena ricostruito può ora essere tradotto in un circuito. Per il modulo $N = 55$, il registro degli esponenti contiene dodici qubit, perché abbiamo scelto $Q = 4096 = 2^{12}$. Il registro dei resti richiede sei qubit: deve rappresentare gli interi da 0 a 54. Eventuali qubit di lavoro si aggiungono a questi due registri.

Il primo registro parte da $|0\rangle$, il secondo da $|1\rangle$. Le porte di Hadamard preparano gli esponenti, il blocco U_f calcola le potenze modulari e la QFT trasforma le ampiezze del primo registro. La misura restituisce un intero y.

Il calcolo delle frazioni continue, la verifica del periodo e la ricerca di d_c avvengono dopo la misura su un computer classico. Il circuito termina quindi prima della decifrazione vera e propria.

Il circuito completo a blocchi



$$U_f|x\rangle|1\rangle \;=\; |x\rangle|13^x \bmod 55\rangle$$

La misura fornisce i dati per il calcolo classico di r e d_c.

Richiami Q è il numero di stati di base del registro degli esponenti. Con n qubit, $Q = 2^n$. Qui $N = 55$, $c = 13$ e $e = 3$.

La preparazione degli esponenti

Una porta di Hadamard trasforma $|0\rangle$ nella sovrapposizione $(|0\rangle + |1\rangle)/\sqrt{2}$. Applicandola separatamente a ogni qubit, ciascun bit dell'esponente assume entrambe le possibilità con la stessa ampiezza.

Con due qubit si ottengono $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$, tutti con ampiezza $1/2$. Con dodici qubit compaiono 4096 termini, ciascuno con ampiezza $1/64$.

$$H^{\otimes 12}|0\rangle = \frac{1}{64}\sum_{x=0}^{4095}|x\rangle$$

La preparazione usa dodici porte. Una misura restituirebbe un solo esponente. Le operazioni successive devono perciò conservare la coerenza delle ampiezze fino all'interferenza di Fourier.

La preparazione con porte Hadamard

$$|0\rangle \longmapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|00\rangle \longmapsto \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

12 qubit : 4096 ampiezze uguali

Richiami La probabilità di uno stato di base è il modulo quadro della sua ampiezza. Qui $|1/64|^2 = 1/4096$.

Le potenze associate ai bit dell'esponente

Per costruire U_f si usa la scrittura binaria dell'esponente. Se $x = x_0 + 2x_1 + 4x_2 + \cdots$, allora ogni bit x_j stabilisce se includere il fattore 13^{2^j}. Le costanti necessarie si calcolano una volta, classicamente, con quadrati successivi modulo 55.

Per esempio, $13^2 \bmod 55 = 4$, poi $4^2 \bmod 55 = 16$ e $16^2 \bmod 55 = 36$. L'esponente $5 = (101)_2$ seleziona le costanti 13 e 16, perché i bit di peso 1 e 4 valgono uno.

$$13^5 \bmod 55 = (13 \cdot 16) \bmod 55 = 43$$

Il numero di costanti cresce con il numero dei bit di x. Anche quando l'esponente è molto grande, non occorre eseguire una moltiplicazione per ciascuna unità del suo valore.

Le costanti delle moltiplicazioni controllate

indice j	potenza 2^j	$13^{2^j} \bmod 55$
0	1	13
1	2	4
2	4	16
3	8	36
4	16	31

Ogni nuova costante è il quadrato della precedente, ridotto modulo 55.

Richiami $x_j \in \{0, 1\}$ è il bit di peso 2^j. Una riduzione modulo 55 può essere eseguita dopo ogni prodotto.

La moltiplicazione modulare reversibile

Una porta quantistica deve essere reversibile. Per una costante a coprima con 55, la moltiplicazione $y \mapsto ay \bmod 55$ permuta i resti: due ingressi diversi non producono la stessa uscita. Il suo inverso moltiplica per $a^{-1} \bmod 55$.

Per esempio, l'inverso di 13 è 17, perché $13 \cdot 17 = 221 \equiv 1 \pmod{55}$. Il passaggio $7 \mapsto 36$ può quindi essere annullato mediante $36 \cdot 17 \bmod 55 = 7$.

Il registro a sei qubit comprende anche gli stati da 55 a 63. Per definire una porta su tutto il registro, possiamo lasciarli invariati. Otteniamo così una permutazione completa dei 64 stati di base, che si estende linearmente alle sovrapposizioni.

La definizione sui 64 stati
e un esempio di inversione

$$U_a|y\rangle = |ay \bmod 55\rangle \quad \text{per } 0 \le y < 55$$

$$U_a|y\rangle = |y\rangle \quad \text{per } 55 \le y < 64$$

$$U_{13} : |7\rangle \longmapsto |36\rangle$$

$$U_{17} : |36\rangle \longmapsto |7\rangle$$

U_{17} annulla l'azione di U_{13}.

Richiami Una permutazione degli stati di base definisce un operatore unitario. La coprimalità garantisce l'esistenza dell'inverso modulare.

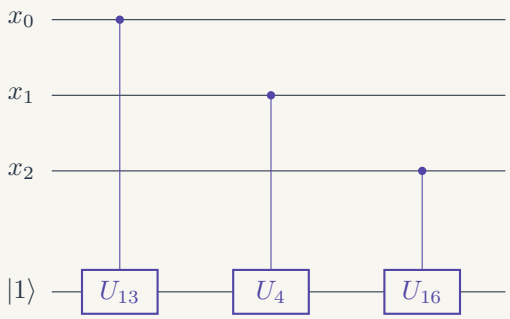
I bit controllano le moltiplicazioni

Il registro dei resti parte da $|1\rangle$, l'elemento neutro della moltiplicazione. Il bit x_0 controlla U_{13}, il bit x_1 controlla U_4, il bit x_2 controlla U_{16} e così via. Quando il controllo vale zero, il registro dei resti rimane invariato.

Il diagramma mostra soltanto i primi tre controlli. Per l'ingresso $x = 5$, le due moltiplicazioni attive producono il resto 43. Per un altro esponente interviene un'altra scelta delle stesse costanti.

La linearità del circuito permette di applicare questa costruzione a una sovrapposizione di esponenti. I controlli conservano x e il registro inferiore raccoglie il valore corrispondente di $f(x)$. La rete realizza quindi la correlazione richiesta dall'algoritmo, senza averne memorizzato in anticipo tutti i valori.

I primi tre bit dell'esponente, dal meno significativo



Per $x = (101)_2 = 5$ agiscono U_{13} e U_{16}: $1 \cdot 13 \cdot 16 \bmod 55 = 43$.

Richiami U_a moltiplica il registro dei resti per a modulo 55. Il controllo attiva la porta soltanto sulla componente con $x_j = 1$.

La pulizia dei registri di lavoro

Le moltiplicazioni reversibili possono richiedere registri temporanei per i riporti e i risultati intermedi. Se il loro contenuto dipende da x, essi rimangono correlati con il registro degli esponenti.

Occorre riportare questi qubit a un valore iniziale comune. Una costruzione generale calcola il risultato in un registro di lavoro, lo trasferisce con porte CNOT in un registro pulito e applica a ritroso il calcolo iniziale. Le CNOT copiano l'etichetta binaria nelle componenti della base, senza clonare uno stato quantistico arbitrario.

Il registro destinato a $f(x)$ conserva l'uscita, mentre i registri temporanei tornano a zero. Questa operazione, detta *uncomputation*, impedisce che residui del calcolo aritmetico alterino l'interferenza prevista.

Il ripristino dei registri ausiliari

$$|x\rangle|0\rangle|0\rangle$$

$$\downarrow$$

$$|x\rangle|w_x, f(x)\rangle|0\rangle$$

calcolo reversibile

$$\downarrow$$

$$|x\rangle|w_x, f(x)\rangle|f(x)\rangle$$

CNOT sui bit del risultato

$$\downarrow$$

$$|x\rangle|0\rangle|f(x)\rangle$$

calcolo inverso sul registro di lavoro

Richiami Un registro ausiliario pulito termina nello stesso stato per ogni x. Il registro di uscita, invece, conserva intenzionalmente la correlazione con $f(x)$.

La QFT e le frazioni binarie

Per costruire la QFT conviene partire da un singolo stato di base. Con due qubit, scriviamo $x = 2x_1 + x_0$. La trasformata distribuisce l'ampiezza sui quattro valori di y, assegnando la fase $e^{2\pi i xy/4}$.

Scrivendo anche $y = 2y_1 + y_0$, il fattore di fase si separa in un contributo per ciascun qubit. Si ottiene il prodotto mostrato a destra: un qubit deve ricevere una fase determinata da x_0, l'altro da entrambi i bit di x.

Le porte di Hadamard producono le sovrapposizioni a due termini. Le rotazioni controllate aggiungono la parte di fase che dipende dagli altri bit. Lo scambio finale riporta i qubit nell'ordine in cui il bit più significativo occupa la linea superiore. La stessa struttura si estende ai registri più lunghi.

La separazione delle fasi sui due qubit

$$x = 2x_1 + x_0, \qquad y = 2y_1 + y_0$$

$$e^{2\pi i xy/4} = e^{\pi i x y_1} e^{\pi i x y_0/2}$$

$$F_4|x\rangle = \frac{|0\rangle + e^{\pi i x_0}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{\pi i (x_1 + x_0/2)}|1\rangle}{\sqrt{2}}$$

Richiami Convenzione adottata: $F_Q|x\rangle = Q^{-1/2} \sum_y e^{2\pi i xy/Q}|y\rangle$. In $|x_1 x_0\rangle$, x_1 è il bit più significativo.

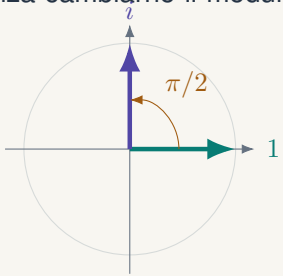
La porta di fase e il suo controllo

La porta R_k lascia invariato $|0\rangle$ e moltiplica l'ampiezza di $|1\rangle$ per $e^{2\pi i/2^k}$. Per $k = 2$ l'angolo è $\pi/2$, perciò il fattore è i. Il diagramma mostra questa rotazione nel piano complesso.

Una fase controllata applica R_k al qubit bersaglio soltanto quando il qubit di controllo vale uno. Per R_2, gli stati $|00\rangle$, $|01\rangle$ e $|10\rangle$ restano invariati, mentre $|11\rangle$ acquista il fattore i.

Le probabilità nella base di calcolo rimangono invariate subito dopo questa porta, perché $|i| = 1$. La variazione emerge quando successive Hadamard fanno interferire componenti con fasi diverse. È così che una rotazione delle ampiezze contribuisce a costruire la trasformata di Fourier.

Una rotazione dell'ampiezza, senza cambiarne il modulo



$$R_2|0\rangle = |0\rangle, \quad R_2|1\rangle = i|1\rangle$$

La fase controllata moltiplica per i soltanto l'ampiezza di $|11\rangle$.

Richiami $R_k = \mathrm{diag}(1, e^{2\pi i/2^k})$. Una fase controllata moltiplica per questo fattore soltanto la componente $|11\rangle$.

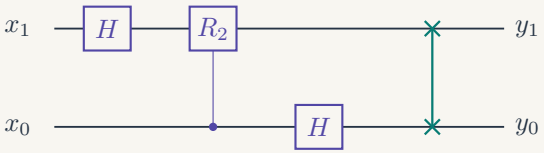
Il circuito della QFT su due qubit

Il circuito si legge da sinistra verso destra. La prima Hadamard agisce sul qubit più significativo x_1. La fase controllata aggiunge alla sua componente $|1\rangle$ il fattore i quando $x_0 = 1$. La seconda Hadamard prepara poi il qubit inferiore.

Prima dello scambio, il qubit superiore contiene la fase dipendente da $x_1 + x_0/2$ e quello inferiore la fase dipendente da x_0. Il prodotto è nell'ordine inverso rispetto alla scomposizione nelle due fasi di uscita. La porta SWAP scambia i qubit e ristabilisce l'ordine convenzionale.

Le etichette y_1, y_0 indicano le posizioni dei bit di uscita. Prima della misura il registro può trovarsi in una sovrapposizione. Il circuito realizza F_4 anche quando l'ingresso è correlato con altri registri.

QFT su 2 qubit: ingresso e uscita nello stesso ordine



$$R_2 \quad = \quad \mathrm{diag}(1, i)$$

Le due croci indicano lo scambio SWAP.

Le operazioni agiscono da sinistra verso destra.

Richiami F_4 usa il segno positivo nell'esponenziale. Lo scambio finale preserva la convenzione $y = 2y_1 + y_0$.

Lo stato uno attraverso la QFT

Seguiamo il circuito per l'ingresso $|01\rangle$, che rappresenta il numero $x = 1$. La prima Hadamard divide l'ampiezza fra $|01\rangle$ e $|11\rangle$. La fase controllata agisce soltanto sul secondo termine, perché solo lì entrambi i bit valgono uno.

La Hadamard inferiore trasforma ciascuna delle due componenti. Quando il bit su cui agisce vale uno, compare il segno meno nella combinazione $(|0\rangle - |1\rangle)/\sqrt{2}$. Infine SWAP scambia $|01\rangle$ con $|10\rangle$.

Le ampiezze finali sono $1/2$, $i/2$, $-1/2$ e $-i/2$. Sono esattamente le quattro fasi della definizione $e^{2\pi i y/4}/2$. Questa verifica rende visibile il contributo di ogni porta. Un singolo stato di base produce probabilità uniformi, mentre la concentrazione dei picchi nasce dalla sovrapposizione periodica degli ingressi.

L'ingresso $|01\rangle$ attraverso tutte le porte

ingresso	$\|01\rangle$
primo H	$\dfrac{\|01\rangle + \|11\rangle}{\sqrt{2}}$
fase controllata	$\dfrac{\|01\rangle + i\|11\rangle}{\sqrt{2}}$
secondo H	$\dfrac{\|00\rangle - \|01\rangle + i\|10\rangle - i\|11\rangle}{2}$
SWAP	$\dfrac{\|00\rangle + i\|01\rangle - \|10\rangle - i\|11\rangle}{2}$

Richiami $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. SWAP scambia i due bit, lasciando invariati $|00\rangle$ e $|11\rangle$.

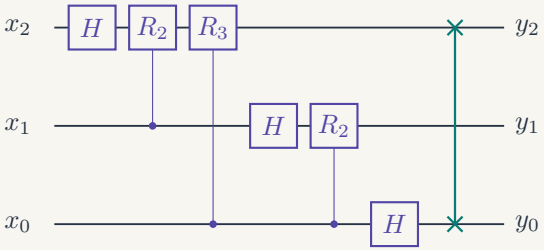
L’estensione a tre qubit

Con tre qubit, il bit più significativo riceve due correzioni di fase: una di angolo $\pi/2$, controllata dal bit centrale, e una di angolo $\pi/4$, controllata dall’ultimo bit. Dopo queste porte si applica la Hadamard centrale, seguita dalla sua fase controllata di angolo $\pi/2$.

La Hadamard inferiore completa la preparazione. Lo scambio fra la linea superiore e quella inferiore restituisce l’ordine y_2, y_1, y_0. Per $|001\rangle$, il risultato ha ampiezze $e^{2\pi i y/8}/\sqrt{8}$: avanzando di uno nel valore di y, la fase ruota di $\pi/4$.

Il circuito conserva quindi la costruzione a due qubit e aggiunge le rotazioni richieste dal nuovo bit. Per linearità, la verifica su tutti gli ingressi della base determina anche l’azione sulle loro sovrapposizioni, comprese quelle periodiche dell’algoritmo.

QFT su 3 qubit: ingresso e uscita nello stesso ordine



$$R_2 = \mathrm{diag}(1, i)$$
$$R_3 = \mathrm{diag}(1, e^{i\pi/4})$$

Le operazioni agiscono da sinistra verso destra.

Richiami $x = 4x_2 + 2x_1 + x_0$. La porta R_3 introduce l’angolo $2\pi/8 = \pi/4$ quando il controllo vale uno.

Il numero delle porte e il risultato disponibile

Su n qubit, la QFT esatta usa n Hadamard e una fase controllata per ogni coppia di linee, dunque $n(n-1)/2$ fasi. Si aggiungono $\lfloor n/2 \rfloor$ scambi per ripristinare l'ordine dei bit. Sono porte logiche ideali, da decomporre nelle operazioni di un dispositivo concreto.

Il costo cresce quadraticamente in $n = \log_2 Q$. L'esponenziazione modulare richiede a sua volta circuiti aritmetici di costo polinomiale nella lunghezza binaria degli ingressi e costituisce una parte sostanziale del lavoro complessivo.

La misura produce un campione della distribuzione. Un numero di ripetizioni polinomiale nella lunghezza dell'ingresso permette, con alta probabilità e controlli classici, di ricostruire il periodo. L'elenco dei Q coefficienti rimane inaccessibile.

Il conteggio delle porte logiche della QFT

$$n = 3$$

3 Hadamard, 3 fasi controllate, 1 SWAP

$$n = 12$$

12 Hadamard, 66 fasi controllate, 6 SWAP

$$n + \frac{n(n-1)}{2} + \lfloor n/2 \rfloor$$

Il numero di porte della QFT esatta cresce come n^2.

Richiami La QFT trasforma $Q = 2^n$ ampiezze con $O(n^2)$ porte logiche. La lettura di tutti i coefficienti non è il risultato offerto dal circuito.

Il calcolo completo sul cifrato tredici

Possiamo ora riunire il percorso aritmetico e la costruzione quantistica. Dai dati pubblici $N = 55$, $e = 3$ e $c = 13$ si costruiscono le costanti modulari e il circuito. Una misura favorevole del registro trasformato può restituire $y = 614$.

Il computer classico interpreta $614/4096$ mediante le frazioni continue e ricava il candidato 20. Le verifiche già descritte stabiliscono che è il periodo delle potenze di 13 modulo 55. L'inverso di 3 modulo 20 è 7, da cui segue il messaggio $13^7 \bmod 55 = 7$.

Una misura diversa può richiedere un'altra esecuzione. Il controllo classico dei candidati fa parte dell'algoritmo. La funzione del circuito è concentrare la probabilità su risultati dai quali queste operazioni efficienti possono estrarre la periodicità necessaria alla decifrazione.

Dati pubblici, misura e decifrazione

$$N = 55, \quad e = 3, \quad c = 13$$

$$\downarrow$$

$$\text{circuito quantistico} \longrightarrow y = 614$$

$$\downarrow$$

$$614/4096 \approx 3/20 \longrightarrow r = 20$$

$$\downarrow$$

$$3 \cdot 7 = 1 + 20 \longrightarrow d_c = 7$$

$$\downarrow$$

$$13^7 \bmod 55 = 7$$

Richiami $r = \mathrm{ord}_{55}(13) = 20$. L'esponente $d_c = 7$ soddisfa $3d_c \equiv 1 \pmod{20}$ e decifra il messaggio considerato.

Le rotazioni molto piccole

Approfondimento facoltativo: QFT approssimata

Aumentando il numero dei qubit, il circuito contiene fasi controllate con angoli sempre più piccoli. Una rotazione R_k ha angolo $2\pi/2^k$: per $k = 10$ è circa $0{,}00614$ radianti. La sua azione è vicina all'identità.

Una QFT approssimata omette le rotazioni inferiori a una soglia scelta in funzione dell'errore ammesso. Poiché gli errori possono accumularsi, la soglia dipende anche dal numero dei qubit. Si deve controllare la variazione complessiva della distribuzione degli esiti.

Il numero intero letto dal registro mantiene la sua precisione binaria. L'approssimazione modifica la probabilità di ottenere un esito utile. Possiamo così ridurre le risorse della QFT senza richiedere un controllo fisico arbitrariamente preciso su ogni piccola rotazione.

Gli angoli diminuiscono con la distanza fra i bit

$$R_2 : \theta = \pi/2$$
$$\downarrow$$
$$R_3 : \theta = \pi/4$$
$$\downarrow$$
$$R_{10} : \theta \simeq 0{,}00614$$
$$\downarrow$$
$$R_k \simeq I \quad \text{per } k \text{ grande}$$

Richiami $R_k = \mathrm{diag}(1, e^{2\pi i/2^k})$. Una QFT approssimata deve controllare l'errore complessivo, oltre a quello delle singole porte.

La QFT seguita immediatamente dalla misura

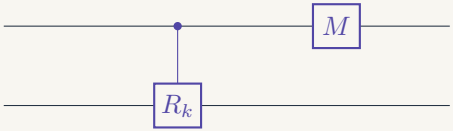
Approfondimento facoltativo: QFT semiclassica

Nella ricerca del periodo tutti i qubit del registro trasformato vengono infine misurati. Una realizzazione semiclassica sostituisce alcune fasi controllate con rotazioni a un qubit, scelte in base a risultati di misura già disponibili.

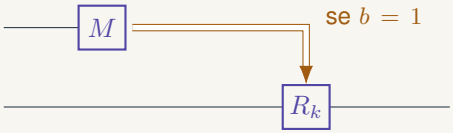
Se un qubit serve soltanto da controllo di una rotazione e poi viene misurato, possiamo misurarlo prima. Quando il risultato è uno applichiamo la rotazione al bersaglio, quando è zero lo lasciamo invariato. I risultati finali hanno la stessa distribuzione.

La sostituzione richiede che il controllo non subisca altre operazioni capaci di mescolarne le componenti. Essa conserva le statistiche della ricerca del periodo, ma non sostituisce una QFT coerente destinata a ulteriori operazioni quantistiche.

Una fase condizionata
al risultato di una misura
Controllo quantistico



Misura anticipata del controllo



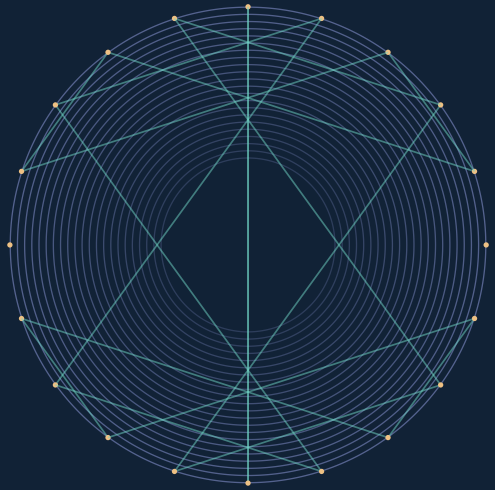
Stessa distribuzione degli esiti finali.

Richiami Il controllo classico usa un risultato di misura già noto. La versione semiclassica è adatta quando la QFT termina con la misura del registro.

APPROFONDIMENTI FACOLTATIVI

Il periodo e i fattori

Un’altra applicazione della ricerca dell’ordine



L’algoritmo di Shor

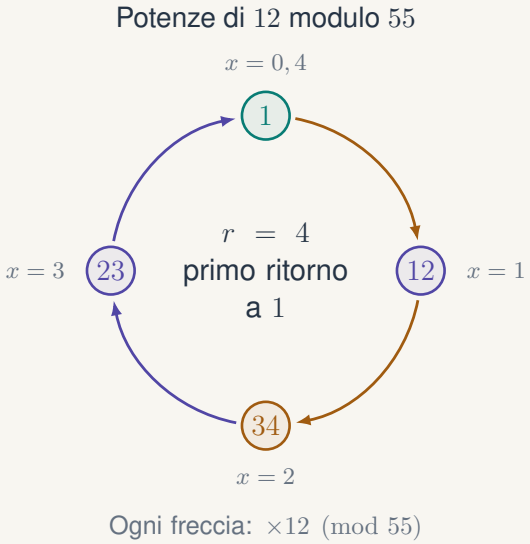
Una base scelta per cercare i fattori

Approfondimento facoltativo

La decifrazione diretta ha usato le potenze del cifrato c. La ricerca del periodo permette anche un'altra applicazione: trovare i fattori del modulo. In questo caso scegliamo noi una base a, senza collegarla a un messaggio intercettato.

Consideriamo ancora $N = 55$ e scegliamo $a = 12$. Il controllo $\mathrm{MCD}(12, 55) = 1$ assicura che le potenze tornino a 1. Se il MCD fosse già un divisore proprio di 55, avremmo trovato un fattore prima del calcolo quantistico.

I resti delle potenze sono $1, 12, 34, 23, 1$. Il periodo minimo vale quindi $r = 4$. La procedura quantistica studiata nei capitoli precedenti può fornirlo anche quando un'esplorazione del ciclo sarebbe troppo lunga.



Richiami Una base coprima soddisfa $\mathrm{MCD}(a, N) = 1$. Il suo ordine r è il primo esponente positivo con $a^r \equiv 1 \pmod{N}$.

Il resto a metà del ciclo

Approfondimento facoltativo

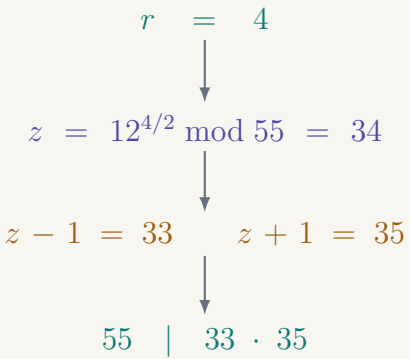
Il periodo $r = 4$ è pari. Possiamo perciò fermarci dopo $r/2 = 2$ passi e chiamare z il resto ottenuto. Nell'esempio $z = 12^2 \bmod 55 = 34$.

Ripetendo due volte questo mezzo percorso completiamo il ciclo. Perciò $z^2 \equiv 1 \pmod{55}$, ossia 55 divide $z^2 - 1$. La differenza di quadrati consente di scrivere la stessa quantità come prodotto:

$$z^2 - 1 = (z-1)(z+1) = 33 \cdot 35.$$

Nessuno dei due numeri 33 e 35 è multiplo di 55, mentre il loro prodotto lo è. I due fattori primi del modulo devono dunque distribuirsi fra queste quantità. Il massimo comun divisore li individua senza dover scomporre 33 o 35 per tentativi.

Il mezzo periodo



Richiami Per un periodo pari, $z = a^{r/2} \bmod N$ soddisfa $z^2 \equiv 1 \pmod{N}$. Qui $34^2 - 1 = 1155 = 21 \cdot 55$.

I due massimi comuni divisori

Approfondimento facoltativo

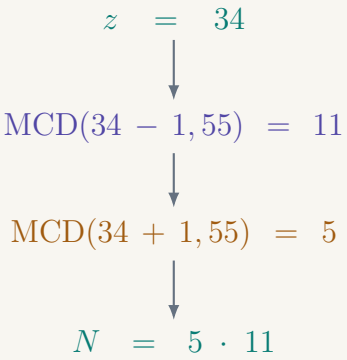
Il calcolo dei fattori è ormai interamente classico. Confrontiamo separatamente $z - 1 = 33$ e $z + 1 = 35$ con il modulo 55. L'algoritmo di Euclide produce:

$$\mathrm{MCD}(33, 55) = 11, \qquad \mathrm{MCD}(35, 55) = 5.$$

Per il primo MCD, dividiamo 55 per 33 e otteniamo resto 22. Dividendo 33 per 22 resta 11, che divide esattamente 22. Per il secondo, i resti successivi sono 20, 15, 5 e infine 0.

Abbiamo così recuperato $55 = 5 \cdot 11$. L'intervento quantistico si è limitato alla ricerca dell'ordine della base scelta. La divisione per due, l'esponenziazione modulare e i MCD richiedono algoritmi classici efficienti nella lunghezza in bit dei numeri.

I fattori del modulo



Richiami Il MCD è il più grande intero positivo che divide entrambi gli argomenti. Un fattore proprio di N è maggiore di 1 e minore di N.

Le condizioni del mezzo periodo

Approfondimento facoltativo

Il passaggio ai fattori richiede un periodo pari e un resto $z = a^{r/2} \bmod N$ diverso da $-1 \bmod N$. Se il periodo è dispari, il mezzo periodo non è un esponente intero. Se $z = -1 \bmod N$, il MCD con $z + 1$ restituisce tutto N, anziché un suo fattore proprio.

Con $N = 55$, la base $a = 16$ ha periodo 5, quindi non consente il primo passaggio. La base $a = 24$ ha periodo 10, ma $24^5 \bmod 55 = 54$, cioè $-1 \bmod 55$. In entrambi i casi scegliamo una nuova base.

Queste condizioni appartengono alla procedura di fattorizzazione. Nell'attacco diretto al cifrato, invece, l'inverso di e modulo il periodo può esistere anche quando il periodo è dispari. Le due applicazioni condividono la ricerca dell'ordine, ma ne usano il risultato in modi diversi.

Due casi distinti

$$a = 16 : \quad r = 5$$

Il mezzo periodo non è intero.

$$a = 24 : \quad r = 10$$
$$24^5 \equiv -1 \pmod{55}$$

In entrambi i casi occorre scegliere una nuova base.

Richiami Per fattorizzare serve r pari e $a^{r/2} \not\equiv -1 \pmod N$. Il minimo periodo esclude già $a^{r/2} \equiv 1$.

La chiave ricostruita dai fattori

Approfondimento facoltativo

Conoscendo $p = 5$ e $q = 11$ possiamo ricostruire una chiave privata valida per tutti i messaggi. Calcoliamo $\varphi(55) = (5-1)(11-1) = 40$ e cerchiamo l'inverso dell'esponente pubblico $e = 3$ modulo 40.

$$3 \cdot 27 = 81 = 1 + 2 \cdot 40.$$

La scelta $d = 27$ consente la decifrazione RSA. Nel percorso principale avevamo recuperato lo stesso messaggio dal cifrato 13 usando il periodo 20 e l'esponente $d_c = 7$, senza conoscere i fattori.

Qui anche 7 funziona come esponente universale, perché ogni ordine modulo 55 divide 20. In generale, però, un cifrato può avere periodo più corto: l'inverso d_c garantisce la decifrazione di quel cifrato, ma può non funzionare per gli altri.

La via della fattorizzazione

$$p = 5, \quad q = 11$$
$$\downarrow$$
$$\varphi(55) = 40$$
$$\downarrow$$
$$3^{-1} \bmod 40 = 27$$
$$\downarrow$$
$$13^{27} \bmod 55 = 7$$

Richiami Chiave: $ed \equiv 1 \pmod{\varphi(N)}$. Attacco diretto: $ed_c \equiv 1 \pmod{\operatorname{ord}_N(c)}$, con $\mathrm{MCD}(c, N) = 1$.

Indicazioni di lettura

N. David Mermin, *Quantum Computer Science: An Introduction*, Cambridge University Press, 2007, capitolo 3, «Breaking RSA Encryption». Le pagine indicate sono quelle stampate nel volume, non il contatore del lettore PDF.

Le pp. 63–69 collegano la ricerca del periodo alla crittografia e mostrano la decifrazione diretta senza fattorizzare il modulo. Le pp. 70–72 introducono i registri e la trasformata di Fourier. Le pp. 79–83 spiegano l'interferenza, la misura e la ricostruzione del periodo.

La costruzione del circuito si trova alle pp. 72–79. Il calcolo della funzione periodica e la tolleranza alle piccole fasi occupano le pp. 83–86. Le pp. 86–87 presentano infine la riduzione della fattorizzazione alla ricerca dell'ordine.

In questa lezione il circuito segue la spiegazione del suo effetto. L'introduzione alle serie di Fourier e i diagrammi numerici preparano la lettura del procedimento discreto. La notazione resta m per il messaggio, e per l'esponente pubblico e c per il cifrato, anche dove il libro adopera lettere diverse.

Richiami Percorso principale: periodo del cifrato, decifrazione, Fourier e circuito. Il collegamento ai fattori costituisce un'applicazione facoltativa.

Fonti sul costo computazionale

Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Journal on Computing 26(5), 1997, pp. 1484–1509. L'articolo analizza l'algoritmo quantistico e il suo costo nella lunghezza in bit dell'ingresso. Versione pubblica: arXiv: quant-ph/9508027.

Dustin Moody e Angela Robinson, *Cryptographic Standards in a Post-Quantum Era*, NIST, 2022, sezione 1. Il confronto introduttivo distingue il costo subesponenziale dei migliori metodi classici generali di fattorizzazione dal costo polinomiale dell'algoritmo di Shor. Documento NIST, identificativo 934896.

Le stime asintotiche descrivono la crescita delle risorse al crescere dell'ingresso. Non misurano i tempi dei piccoli esempi della lezione e non prevedono quando sarà disponibile un dispositivo capace di attaccare un modulo RSA di dimensione crittografica.

Richiami Non è nota una dimostrazione generale di impossibilità di un algoritmo classico efficiente per la fattorizzazione. Il confronto riguarda algoritmi conosciuti.