90-quantum-shor-arithmetic-background-04

Quantum Computing

Algoritmo di Shor

Background e overview

1

1

il problema della fattorizzazione

- dato un numero intero positivo N vogliamo scomporlo in fattori primi, cioè vogliamo scrivere $N = {p_1}^{e_1} \cdot {p_2}^{e_2} \cdots {p_k}^{e_k}$ dove $p_1 \cdots p_k$ sono i numeri primi divisori di N
  - es: se $N = 120$ vogliamo scrivere $N = 2^3 \cdot 3^1 \cdot 5^1$

2

2

un caso difficile e RSA

- il problema della fattorizzazione è particolarmente difficile quando $N = P \cdot Q$ dove P e Q sono numeri primi di dimensioni simili
  - proprio su questa difficoltà si fonda il cryptosystem RSA, alla base della sicurezza delle nostre transazioni e dei nostri acquisti on-line
- RSA sfrutta il fatto che fattorizzare un numero richiede molto tempo
  - attualmente, per ciò che riguarda il calcolo classico, sono noti solo algoritmi con complessità *esponenziale*

3

3

complessità esponenziale in cosa?

- se n è il numero di bit usati per rappresentare N, allora l'algoritmo più ovvio per la fattorizzazione impiega un tempo $O(N) = O(2^n)$
- l'algoritmo più efficiente attualmente noto ha complessità $2^{O(\sqrt[3]{n})}$, ancora esponenziale
- ciò rende attualmente impossibile usare algoritmi classici per fattorizzare numeri con un migliaio di bit

4

4

un po' di aritmetica modulare

- l'espressione $a \equiv b(\text{mod } N)$ indica che esiste un q tale che $b = qN + a$
- ad esempio abbiamo
  - $3 \equiv 24(\text{mod } 21)$
  - $2 \equiv 44(\text{mod } 21)$
- ma anche
  - $20 \equiv -1(\text{mod } 21)$

5

5

addizioni e moduli

- l'espressione $a \equiv b(\text{mod } N)$ indica che esiste un q tale che $b = qN + a$
- esempio
  - $24 + 35(\text{mod } 21) \equiv 3 + 14(\text{mod } 21) \equiv 17(\text{mod } 21)$

6

6

moltiplicazioni e moduli

- l'espressione $a \equiv b (\mathrm{mod}\ N)$ indica che esiste un q tale che $b = qN + a$
- esempio
  - $24 \cdot 30 (\mathrm{mod}\ 21) \equiv 3 \cdot 9 \equiv 27 \equiv 6 (\mathrm{mod}\ 21)$
- i calcoli dell'aritmetica modulare si possono svolgere in modo *efficiente*

7

7

massimo comun divisore

- il massimo comun divisore $\gcd(x, y)$ tra due numeri x e y può essere calcolato in modo efficiente, usando l'algoritmo di Euclide
  - senza fattorizzare i due numeri
- $\gcd(x, y)$

  while $y \neq 0$

    set $z = y$

    calcola $y \equiv x (\mathrm{mod}\ y)$

    set $x = z$

  return x

8

8

90-quantum-shor-arithmetic-background-04

un modo per fattorizzare un numero

- per fattorizzare N una buona idea è quella di cercare un numero x tale che $x^2 \equiv 1 (\mathrm{mod}\ N)$
  - es. se vogliamo fattorizzare 21 possiamo cercare di risolvere $x^2 \equiv 1 (\mathrm{mod}\ 21)$
  - soluzioni banali: $x = 1$ e $x = -1$
  - una soluzione non banale è $x = 8$, infatti $x^2 = 64 \equiv 1 (\mathrm{mod}\ 21)$
  - possiamo scrivere $8^2 \equiv 1 (\mathrm{mod}\ 21)$ e $8^2 - 1^2 \equiv 0 (\mathrm{mod}\ 21)$
  - quindi 21 divide senza resto $8^2 - 1^2 = (8+1)(8-1)$

9

9

un modo per fattorizzare un numero

- per fattorizzare N una buona idea è quella di cercare un numero x tale che $x^2 \equiv 1 (\mathrm{mod}\ N)$
  - quindi 21 divide senza resto $8^2 - 1^2 = (8+1)(8-1)$
  - nota come 21 non divida né $(8+1)$ né $(8-1)$ ma il suo divisore 3 divide $(8+1)$ e il suo divisore 7 divide $(8-1)$
  - quindi c'è un divisore comune tra 21 e $(8+1)$ e tra 21 e $(8-1)$
  - sono entrambi divisori di 21 e per cercarli efficientemente basta calcolare $\gcd(21, (8+1))$ e $\gcd(21, (8-1))$

10

10

un modo per fattorizzare un numero

- per fattorizzare N una buona idea è quella di cercare un numero x tale che $x^2 \equiv 1 (\mathrm{mod}\ N)$
- se troviamo un $x \not\equiv \pm 1 (\mathrm{mod}\ N)$ e che soddisfa $x^2 \equiv 1 (\mathrm{mod}\ N)$ riusciamo a fattorizzare N facilmente perché sappiamo che N divide senza resto $x + 1$ e $x - 1$
- il fatto che $x \not\equiv \pm 1 (\mathrm{mod}\ N)$ implica $x \pm 1 \not\equiv 0 (\mathrm{mod}\ N)$ e che quindi N non divida $x \pm 1$
- quindi N e $x + 1$ hanno un divisore comune e per cercare un divisore di N basta fare $\gcd(N, x + 1)$

11

11

esempio – x tale che $x^2 \equiv 1 (\mathrm{mod}\ N)$

- supponiamo $N = 100$
  - cerchiamo x tale che $x^2 \equiv 1 (\mathrm{mod}\ 100)$
  - abbiamo che $49^2 = 2401 \equiv 1 (\mathrm{mod}\ 100)$
  - quindi $49^2 - 1 \equiv 0 (\mathrm{mod}\ 100)$
  - allora $(49 - 1)(49 + 1) \equiv 0 (\mathrm{mod}\ 100)$
  - quindi 48 e 50 hanno un divisore in comune con 100, si tratta di 4 e 50, li troviamo efficientemente calcolando $\gcd(100,48)$ e $\gcd(100,50)$
- non è stato facile trovare 49, ma una volta trovato, il problema è stato risolto!

12

12

come risolvere $x^2 \equiv 1(\text{mod } N)$?

- supponiamo ancora $N = 21$ e scegliamo un numero random, es. $x = 2$; definiamo la tabella
  - $2^0 \equiv 1(\text{mod } 21)$
  - $2^1 \equiv 2(\text{mod } 21)$
  - $2^2 \equiv 4(\text{mod } 21)$
  - $2^3 \equiv 8(\text{mod } 21)$
  - $2^4 \equiv 16(\text{mod } 21)$
  - $2^5 \equiv 11(\text{mod } 21)$
  - $2^6 \equiv 1(\text{mod } 21)$ che è anche $(2^3)^2 \equiv 1(\text{mod } 21)$, quindi 8 è una soluzione non banale per l'equazione

13

13

come risolvere $x^2 \equiv 1(\text{mod } N)$?

- un algoritmo potrebbe quindi essere: scelgo un numero random x e provo a calcolare
  - x^0
  - x^1
  - …
  - $x^r \equiv 1(\text{mod } N)$
- sperando di trovare un numero r tale che: r è pari, $(x^{r/2})^2 \equiv 1(\text{mod } N)$ e $x^{r/2} \not\equiv \pm 1(\text{mod } N)$
- se lo troviamo abbiamo trovato una soluzione non banale all'equazione

14

14

quanto è probabile che x funzioni?

- lemma: sia N un numero intero positivo con almeno due fattori primi distinti e sia x un numero random scelto in modo uniforme tra 0 e $N-1$; se $\gcd(x,N)=1$ allora con probabilità almeno $1/2$ il minimo r tale che $(x^{r/2})^2 \equiv 1 (\mathrm{mod}\ N)$ è pari ed è tale che $x^{r/2} \not\equiv \pm 1 (\mathrm{mod}\ N)$

15

15

e se $\gcd(x,N) \neq 1$?

- è ancora meglio: il divisore comune di x ed N è anche un divisore di N

16

16

90-quantum-shor-arithmetic-background-04

dato un certo x (ed N), come trovare r?

torniamo all'esempio con $N = 21$ e $x = 2$ e alla tabella

a	$f(a) = x^a \pmod N$
0	1
1	2
2	4
3	8
4	16
5	11
6	1
7	2
8	4
9	8
10	16
11	11
12	1
13	2
14	4

la funzione è periodica con periodo $r = 6$

se troviamo il periodo troviamo r tale che $(x^{r/2})^2 \equiv 1 \pmod N$ e se r è pari abbiamo risolto

17

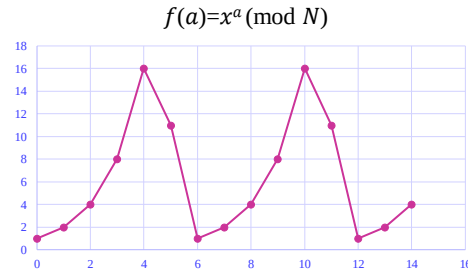
17

dato un certo x (ed N), come trovare r?

a	$f(a) = x^a \pmod N$
0	1
1	2
2	4
3	8
4	16
5	11
6	1
7	2
8	4
9	8
10	16
11	11
12	1
13	2
14	4

la funzione è periodica con periodo $r = 6$

se troviamo il periodo troviamo r tale che $(x^{r/2})^2 \equiv 1 \pmod N$ e se r è pari abbiamo risolto



18

18

funzioni periodiche

- una funzione f è *periodica* quando per qualche $r > 0$ e per ogni x abbiamo $f(x + r) = f(x)$

19

19

es: – compila la tabella $f(a) = x^a \pmod N$

torniamo all'esempio con $N = 100$ e supponiamo di aver randomizzato $x = 9$; compiliamo la tabella

a	$f(a) = x^a \pmod N$
0	1
1	9
2	81
3	29
4	61
5	49
6	41
7	69
8	21
9	89
10	1
11	9
12	81
13	29
14	61

la funzione è periodica con periodo $r = 10$

se troviamo il periodo troviamo r tale che $(x^{r/2})^2 \equiv 1 \pmod N$ e se r è pari abbiamo risolto

qui r è pari e abbiamo $(9^{r/2})^2 = (9^{10/2})^2 = (59049)^2 = 9^{10} = 3486784401$

20

20

algoritmo

- input: N con almeno due fattori primi distinti
- output: un divisore di N
  - scegli in modo uniforme un numero x random tra 0 e $N-1$
  - se $\gcd(x,N) \neq 1$ allora il divisore comune di x ed N è anche un divisore di N
  - altrimenti, calcola il periodo r della funzione $f(a) = x^a \pmod N$; se r è pari ed è tale che $(x^{r/2})^2 \equiv 1 \pmod N$ allora il divisore è $\gcd(N, x+1)$; altrimenti riprova con un altro x

21

21

analisi e problemi da affrontare

- gcd si calcola in modo efficiente
- visto il lemma, il numero di tentativi da fare non è troppo alto
- il problema è che purtroppo il periodo r può avere una dimensione simile a quella di N
  - per calcolare il periodo in modo efficiente usiamo la Discrete Fourier Transform (DFT) rivisitata in termini quantistici (QFT)

22

22