Fattorizzazione di interi

1. Fermat

Sia n intero dispari

se $n = ab$ allora

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a+b}{2}\right)^2 = t^2 - s^2$$

ossia n è differenza di quadrati.

Per $t = \lceil \sqrt{n} \rceil + 1, \dots, n-1$ si considera

$$t^2 - n$$

fino a quando si trova un quadrato

$$t^2 - n = s^2$$

Allora $n \mid t^2 - s^2 = (t+s)(t-s)$

e $d = \gcd(n, t-s) = \begin{cases} 1 \\ n \\ p^s \cdot r \\ q \end{cases}$

Se $n = p^k q$ p primo
$(p, q) = 1$

Se $s \not\equiv \pm t \ (n)$, $\gcd(n, s-t) \neq 1, n$

Infatti

- $\gcd(n, s-t) = 1 \Rightarrow \gcd(n, t+s) = n$
  ossia $t \equiv -s \ (n)$

- $\gcd(n, s-t) = n \Rightarrow t \equiv s \ (n)$

$=$

Quindi si fattorizza n.

$\therefore$ Se n piccolo ok

In generale può difficile che

$t^2 - n$ sia un quadrato

perfetto

Modifico

Esempio: $n = 1649$ $\lceil\sqrt{n}\rceil = 41$

Se consideriamo

$$t^2 \equiv s^2 \ (n) \quad \text{e troviamo } t = 41, 42, 43$$

si ha

$$(41)^2 \equiv 32 \ (n)$$

$$(42)^2 \equiv 115 \ (n)$$

$$(43)^2 \equiv 200 \ (n)$$

ossia <u>nessuno</u> dei valori è un quadrato. Però:

$$80^2 = 32 \cdot 200 \equiv (41)^2 \cdot (43)^2 = (41 \cdot 43)^2 \ (n)$$

Così $80^2 \equiv (41 \cdot 43)^2 \equiv (114)^2 \ (n)$

Da cui $(114 + 80)(114 - 80) \equiv 0 \ (n)$

$\gcd(n, 34) = 17 \ldots$

∴ Dato un insieme di interi trovarne uno si il cui prodotto sia un quadrato!

<u>Esempio</u> $n = 1649$

$(41)^2 \equiv 32 = 2^5 \quad (n)$

$(42)^2 \equiv 115 = 5 \cdot 23 \quad (n)$

$(43)^2 \equiv 200 = 2^3 \cdot 5^2 \quad (n)$

Dato $\{ 2^5, \ 5 \cdot 23, \ 2^3 \cdot 5^2 \}$

quale sottoinsieme scegliere?

le basi sono $2, 5, 23$ associamo a ogni elemento il vettore degli esponenti di $2, 5, 23$

$$2^5 \longrightarrow (5,0,0) \qquad 5 \cdot 23 \rightarrow (0,1,1) \qquad 2^3 5^2 \rightarrow (3,2,0)$$

$$\downarrow \text{mod } 2 \qquad\qquad \downarrow \text{mod } 2 \qquad\qquad \downarrow (2)$$

$$(1,0,0) \qquad\qquad (0,1,1) \qquad\qquad (1,0,0)$$

e cerchiamo quali vettori sono lin. dip su F_2

la dipendenza lineare su F_2 equivale a dire che la somma degli esponenti è pari, ossia che il prodotto è un quadrato

$$(41)^2(43)^2 \equiv \underbrace{2^5 \cdot 2^3}\cdot 5^2 = 2^8 \cdot 5^2 = (2^4 \cdot 5)^2 \quad (n)$$

Però in general i primi che intervengono nelle fattorizzazioni sono molti e diversi, quindi la matrice troppo grande

Allora scegliamo dei valori per t in modo che $t^2 - n$ abbia solo fattori primi piccoli! (numerilisci)

I numeri lisci sono più difficili da trovare, ma così vettori più piccoli e matrici di dimensioni piccole

---

Il crivello quadratico ci aiuta a trovare i numeri lisci.

Vediamo intanto come trovare elementi s_i tali che $\prod s_i$ sia un quadrato.

Basi di fattori

<u>Definizione</u> Chiamiamo un insieme $B = \{-1, p_2, \dots, p_h\}$ con p_i primi distinti una <u>base di fattori</u>.

Diciamo che b è un B-numero (dato n) se $b^2 \equiv \beta \ (n)$ $-\frac{n}{2} < \beta \leq \frac{n}{2}$ e $\beta = \prod_{p_i \in B} p_i^{a_i}$

<u>Es.</u> $n = 1649$ $\quad B = \{-1, 2, 3\}$

$b = 41$ è un B.numero $b^2 \equiv 41^2 = 32 \ (n)$

$m = 44$ <u>non è</u> un B.numero dato che

$$(44)^2 \equiv 287 = 7 \cdot 41 \ (n)$$

Fissata una base di fattori B facciamo corrispondere a ogni B-numero il vettore degli esponenti mod 2

$$b^2 = \prod p_i^{a_i} \ (n) \longrightarrow e = (\bar{\alpha}_1, \dots, \bar{\alpha}_n) \qquad \bar{\alpha}_i \equiv \alpha_i \ (2)$$

Come nell'esempio:

Se $b_1^2 \dots b_r^2$ sono B-numeri $\displaystyle b_i^2 = \prod_{p_j \in B} p_j^{a_{ij}} \ (n)$

$$\downarrow$$

$$e_1 + \dots + e_r \equiv \underline{0} \ (2)$$

$$\Updownarrow$$

$$(\underbrace{\Sigma a_{1j}}_{2\gamma_1}, \dots, \underbrace{\Sigma a_{rj}}_{2\gamma_r}) \equiv 0 \ (2)$$

Allora $b = \prod b_i \ (n)$ $\qquad c = \prod_{p_i \in B} p_i^{\gamma_i} \ (n)$ (bilanciata)

sono t.c

$$b^2 \equiv c^2 \ (n)$$

Oss. Se $b \equiv \pm c \ (n)$ bisogna cercare altri B-numeri

Quanti b_i dobbiamo trovare?

Se $B = \{-1, p_2, \dots, p_h\}$ $\quad$ $h+1$ bastano!

Nota In generale per b_i scelti random e n composto $b \equiv \pm c \ (n)$ al più per $1/2$ delle scelte.

Infatti se n ha r fattori primi ogni quadrato ha $2^r \geq 4$ radici quadrate e quindi una radice random di b^2 ha solo

$$\frac{2}{2^r} \leq \frac{1}{2}$$

possibilità di essere b o $-b$

Come scegliere la base di fattori e i b_i?

In pratica si parte con i primi h primi (tali che $\left(\frac{n}{p}\right)=1$) e b_i random.

Oppure scegliere i b_i tc $b_i^2(n)$ (LAR) è piccolo. Es $b_i \simeq \sqrt{kn}$ k piccoli.

Stima del tempo

- $O\left(e^{c\sqrt{z \log z}}\right) = O\left(e^{c\sqrt{\log n \log\log n}}\right)^*$

con $c = 1+\varepsilon$

meglio di Pollard per n grandi

$$O(\sqrt[4]{n}) = O(e^{cz}) \quad c = \frac{1}{4}\log 2$$

* Stima per algoritmi veloci

($\neq$ number field sieve).

Crivello quadratico

Variante del metodo precedente

$B = \{ p \mid p \leq P, \left(\frac{n}{p}\right) = 1, \text{dispari} \} \cup \{2\}$

$S = \{ t^2 - n \mid \lfloor \sqrt{n} \rfloor + 1 \leq t \leq \lceil \sqrt{n} \rceil + A \}$

dove P e A Bound "opportuni"

<u>Differenza</u>

<u>Factor Base</u>	<u>QS</u>
$\forall s \in S$ si divide per i primi di B per vedere se B-numero	si sceglie p e si verifica la divisibilità per tutti gli S simultaneamente

Algoritmo

1. Si sceglie un ~~limite~~ bound P.

$h = \# B$ controlla la lunghezza dei vettori e le dimensioni della matrice degli esponenti

2. Si usa il crivello per trovare $h+1$ numeri b_i t.c. $b_i^2 = a_i \ (n)$ è B-liscio

3. Si fattorizzano a_i e si generano i vettori degli esponenti

4. Si calcolano gli esponenti e le relazioni e $b = \prod b_i \ (n)$ e $a^2 = \prod a_i$

quadrato liscio

5. Da $a^2 \equiv b^2 \ (n)$ si calcolano radici

6. $\gcd(n, a+b)$, $\gcd(n, a-b)$

se n o 1 Ripetere.

Crivello.

Dobbiamo "selezionare" tra gli elementi della forma $t^2 - n$ i B-numeri.

Scriviamo $t = \lfloor \sqrt{n} \rfloor + x$

e quindi cerchiamo x e $y(x)$

con $y(x) = (\lfloor \sqrt{n} \rfloor + x)^2 - n$

in questo modo (se x piccolo)

$$y(x) = (\lfloor n \rfloor + x)^2 - n$$

$$\simeq 2x \lfloor \sqrt{n} \rfloor$$

Osservazione

Se $f(x) = x^2 - n$ allora

$$f(x+kp) = x^2 + (kp)^2 + 2kpx - n$$

$$\equiv x^2 - n = f(x) \ (p)$$

Quindi se α è t.c. $f(\alpha) \equiv 0 \ (p)$

anche $f(\alpha + kp) \equiv 0 \ (p)$

→ Applicando a $y(x) = (x + \sqrt{|n|})^2 - n$

Sia $p \in B$

1. Risolviamo

$$(x + (\sqrt{|n|}))^2 \equiv n \ (p)$$

2. Se α è radice allora

$$y(\alpha) \equiv y(\alpha + p) \equiv \dots \equiv y(\alpha + kp) \equiv 0 \ (p)$$

3. dividiamo allora tutti questi elementi per p

4. Ripetiamo $\forall p \in B$ questo procedimento i valori di y che alla fine sono 1 corrispondono ai b_i buoni!

ES. Sia $n = 15347$, $B = \{2, 17, 23, 29\}$ $\left(\frac{n}{p}\right) = 1 \ \forall p \in B$

Scegliamo di applicare il crivello ai primi 100 numeri della forma $t = \lceil\sqrt{n}\rceil, \lceil\sqrt{n}\rceil + 1, \dots, \lceil\sqrt{n}\rceil + 99$

Definiamo $y(x) = (x + \lceil n \rceil)^2 - n = (x+124)^2 - n$

e $v = (y(0), y(1), y(2), y(3), y(4), \dots, y(71), \dots, y(99))$

$= (29, 278, 529, 782, 1037, \dots, 22678, \dots, 34382)$

Sia $p = 2$. Risolviamo $(x+124)^2 \equiv n \ (2)$

troviamo 1 radice $\alpha \equiv 1 \ (2)$

Allora tutti i valori $y(1+2k) \equiv 0 \ (2)$

Dividendo per 2 ~~[illegible]~~ gli el. in v corrispondenti

$v = (29, 139, 529, 391, 1037, \dots, 11339, \dots, 17191)$

$p = 17$. In questo caso $(x+124)^2 \equiv n \ (17)$ 2 radici!

$\alpha \equiv 3 \ (17)$, $\beta \equiv 4 \ (17)$.

Dividendo per 17 gli elementi della forma $y(3 + k17)$ e $y(4 + k17)$ otteniamo

$v = (29, 139, 529, 23, 61, \dots, 669, \dots, 17191)$

$p=23$ le radici sono $\alpha\equiv 2$, $\beta=3$ e quindi

$$v=(29,139,23,1,61,\dots,29,\dots,17191)$$

$p=29$, $\alpha\equiv 0$ e $\beta=13$. Da cui

$$v=(\overset{y(0)}{1},139,23,\overset{y(3)}{1},61,\dots,\overset{y(71)}{1},\dots,17191)$$

Quindi i valori di t lisci sono

$$t=x+\sqrt{\lceil n\rceil}=x+124=124,127,195$$

per questi valori t^2-n è un quadrato esprimibile con numeri piccoli $\in$ e anche un B-numero perché

$p\in B$.

Fattorizzando (es. con Pollard) si ottiene

$$s_1=29=2^0\cdot 17^0\cdot 23^0\cdot 29\longrightarrow(0,0,0,1)\text{ esp.}$$
$$s_2=782=2^1\cdot 17^1\cdot 23^1\cdot 29^0\longrightarrow(1,1,1,0)$$
$$s_3=22678=2^1\cdot 17^1\cdot 23^1\cdot 29^1\longrightarrow(1,1,1,1)$$

Se risolviamo il sistema

su $\mathbb{Z}/2$

$$Z \cdot \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} = \underline{0}$$

si ha $Z=(1,1,1)$ e quindi

il prodotto

$$S_1 \cdot S_2 \cdot S_3 = 29 \cdot 782 \cdot 22678$$
$$= (22678)^2$$

è un quadrato (in $\mathbb{Z}$)

Da questo otteniamo che

$$124^2 \cdot 127^2 \cdot 195^2 = (3070860)^2$$
$$\equiv 22678^2 \quad (n)$$

Calcolando

$$\gcd(3070860 - 22678, n) = \underline{\underline{103}}$$

Fattore non banale di n

Osservazioni

1. Dato che $\# B = 4$ avremmo dovuto trovare 5 valori per gli s_i, per essere sicuri di trovare una relazione fra gli esponenti. Ma "spesso" come in questo caso ne bastano meno.

2. Abbiamo "perso" le informazioni sui $p \in B$ che dividono gli s_i

3. Tra i valori "finali" di $v = (1, 139, 23, 1, \ldots)$ c'è ancora un elemento divisibile per 23. Avremmo potuto trovare (dividendo per 23) che $y(2) = 529 = 23^2$ e quindi (dato che $23^2 \xrightarrow[(2)]{} (0,0,0,0)$)

$$y(2) = 529 = (126)^2 \equiv 23^2 \, (n) \quad e$$

$$\gcd(126 - 23, n) = \underline{\underline{103}}$$

Per "risolvere" il punto 2. basta ricordarsi delle divisioni che si fanno ad esempio costruendo una tabella

$t = x + \lceil \sqrt{n} \rceil$	y	p_1	p_2	$\dots$	p_k	y iniziale (non si cambia)
$\sqrt{n}$	$y(0)$	0	0	$\dots$	0	$y(0)$
$\sqrt{n}+1$	$y(1)$	0	0	$\dots$	0	$y(1)$
$\sqrt{n}+2$	$y(2)$	0	0	$\dots$	0	$y(2)$
$\vdots$	$\vdots$					$\vdots$

e durante l'esecuzione del crivello aggiornando i valori y (dividendo per il p considerato) e mettendo un 1 nella colonna di p.

Nel nostro esempio alla fine otteniamo

t	y	2	17	23	29	y iniziale (NON si cambia!)
124	1	0	0	0	1	29
127	1	1	1	1	0	782
195	1	1	1	1	1	22678

(ho riportato solo i valori di $y = 1$)

Vediamo ora come usare la divisibilità per potenze superiori di $p \in B$ (punto 3) e quindi individuare potenzialmente un numero maggiore di B-numeri.

Siano $B = \{p_1, \dots, p_h\}$ la base di fattori, $t = \lceil n \rceil, \dots, \lceil n \rceil + A$ i valori su quali fare il crivello:

Sieve:

1. for $p \in B$ p, dispari repeat

   1. Calcola le radici $\alpha \not\equiv \beta\ (p)$ dell'equazione $y(x) \equiv (\underbrace{x + \lceil n \rceil}_{t})^2 - n \equiv 0\ (p)$

   2. Semplifica la tabella: dividi per p i valori $y(\alpha + kp)$ e $y(\beta + kp)$ (per $\alpha + kp \leq A$); aggiungi 1 al valore nella colonna p in corrispondenza agli $y(\alpha + kp)$, $y(\beta + kp)$

3.

3. for $s = 2, 3, \ldots$ repeat

   Calcola α_s e β_s soluzioni (** dopo)

   di $y(x) \equiv 0 \quad (p^s)$

4. Se $\alpha, \beta > \lceil \sqrt{n} \rceil + A \Rightarrow$ vai al primo successivo

   altrimenti "semplifica" la tabella come in 2.

b. Controlla la divisibilità (e semplifica) per potenze di 2 degli elementi $y(x) \neq 1$. (facile)

(continuazione)

Esempio: consideriamo $p = 23$

Risolviamo $f(x) \equiv 0 \ (23)$, $\alpha \equiv 2$, $\alpha \equiv 3 \ (23)$

allora la tabella "semplificata" è

x	y	23
0	29	0
1	278	0
2	$\frac{529}{23} = 23$	1
3	$\frac{782}{23} = 34$	1
	$\vdots$	$\vdots$
25	$\frac{6854}{23} = 298$	1
26	$\frac{7153}{23} = 311$	1
$\vdots$		$\vdots$

Risolviamo ~~per~~ $f(x) \equiv 0 \ (23^2)$, $\alpha \equiv 2$, $\beta \equiv 279 \ (23^2)$

$\beta = 279$. $\alpha \leq 100$ quindi va bene e possiamo "semplificare" i valori $f(\alpha + kp^2)$ nel nostro intervallo: dato che $p^2 = 259$ solo per $k = 0$.

Mentre $\beta > 100$ quindi non otteniamo informazioni.

Nota che $\beta = 279 \equiv 3 \ (23)$ ossia β "corrisponde" alla radice 3 trovata prima

$\alpha+\lceil M\rceil$ è uno dei valori su cui stiamo facendo il crivello e possiamo semplificare gli elementi

$$\underline{y(\alpha+kp^2)}\ \ \underline{\text{per } P}. \quad (\text{se } \alpha+kp^2 \leq 100)$$

(nota che $\beta = 279 \equiv 3\ (23)$)

Dato che $p^2 = 259$ dividiamo solo $y(2)$ e otteniamo

x	y	23
⋮	⋮	0
		0
2	1	2
3	34	1
	⋮	

la tabella è aggiornata:

x	y	... 23 ...
0	29	0
1	278	0
2	$\frac{23}{23} = 1$	2
3	34	1
⋮		⋮
25	298	1
26	311	1

allora $y(2) = 529$ è un B-numero.

Oss. Abbiamo usato il polinomio $y(t)=t^2-n$ ma in pratica se ne usano molti diversi perché uno solo non genera abbastanza B-numeri. I polinomi usati devono essere quadrati mod n e quindi $y(t)=(at+b)^2-n$. Se $b^2-n=ac$ e a è un quadrato basta allora $y(t)=(at^2+2bt+c)$. FACILE PARALLELIZZAZIONE!

ii. <u>Problema</u>: Calcolare le soluzioni di $x^2 \equiv n \ (p^k)$, $k \geq 1$ (se $\left(\frac{n}{p}\right) = 1$)

Sia <u>P dispari</u>

- se $k = 1$ ok Cipolla, Tonelli-Shanks
- se $k > 1$ possiamo usare il lemma di Hensel.

Due forme:
1) Hensel lineare
2) Hensel quadratico

1. <u>Hensel lineare</u>.

Sia $f(x) \in \mathbb{Z}[x]$, p primo e x_1 t.c.

$f(x_1) \equiv 0 \ (p)$ e $f'(x_1) \not\equiv 0 \ (p)$

Allora $\forall k \geq 1$, posto

$$x_{k+1} \equiv x_k - \left[f'(x_1)\right]_p^{-1} \cdot f(x_k) \quad (p^{k+1})$$

inverso di $f'(x_1)$ mod p

Si ha che $f(x_{k+1}) \equiv 0 \ (p^{k+1})$

<u>Traccia dim.</u> Per $n=2$. Sia x_1 t.c. $f(x_1)\equiv 0\ (p)$ e $f'(x_1)\not\equiv 0\ (p)$ e poniamo $x_2 = x_1 + pX$. Usando Taylor si ha

$$f(x_2) \equiv f(x_1) + p\cdot X\cdot f'(x_1)\ \ (p^2)$$

quindi imponendo che $f(x_2)\equiv 0\ \ (p^2)$ e ricordando che $f(x_1)\equiv 0\ \ (p)$ si ha

$$-\frac{f(x_1)}{p} \equiv X\cdot f'(x_1)\ \ (p)$$

Da cui $X \equiv -\frac{f(x_1)}{p}\cdot\left[f'(x_1)\right]_p^{-1}$

sostituendo

$$x_2 = x_1 + pX \equiv x_1 - \left[f'(x_1)\right]_p^{-1}\cdot f(x_1)\ \ (p^2)$$

In modo analogo si costruisce x_{k+1} da x_k ricordando che per ipotesi induttive e costruzione

$$x_k \equiv x_1\ \ (p)$$

$$f(x_k) \equiv 0\ \ (p^k).$$

<u>OSS</u>. Nel nostro caso se p è dispari

certamente $\quad y'(\alpha) = 2\,(x + \lceil\sqrt{n}\,\rceil) \not\equiv (p)$

per α t.c. $\quad y(\alpha) = (\alpha + \lceil\sqrt{n}\,\rceil)^2 - n \equiv 0\ (p)$

<u>Es</u> (continua) per $p = 23 \quad \alpha \equiv 2\ (23)\,,\ \beta \equiv 3\ (23)$

sono le radici di $\quad y(x) = (x + \lceil\sqrt{n}\,\rceil)^2 - n \equiv 0\ (23)$

$$\equiv (x + 124)^2 - n \equiv 0$$

Si ha $\quad y'(x) = 2\cdot(x+124)$.

Consideriamo $\quad \alpha \equiv 2\ (23)\,,\quad y'(\alpha) = 254$

$y'(\alpha)^{-1} \equiv 254^{-1} \equiv 8\ (23)\quad$ quindi

$$\alpha_2 \equiv \alpha - y(\alpha)\cdot\left[y(\alpha)\right]_{23}^{-1} \equiv$$

$$\equiv 2 - 529\cdot 8 \equiv -4230 \equiv 2\ (23^2)$$

Se $\beta \equiv 3 \quad y'(\beta) = 254 \equiv +1\ (23)$

$$\beta_2 \equiv 3 - y(\beta)\cdot\left[y'(\beta)\right]_{23}^{-1} \equiv$$

$$\equiv 3 - 782 \equiv -779 \equiv 259\ (23^2)$$

e quindi le radici mod 23^2 sono

$$\alpha_2 \equiv 3 \quad e \quad \beta_2 = 259$$

2 Sollevamento quadratico (Cfr. Childs - Introduction to Higher Algebra).

Siano, $p \in \mathbb{Z}$, $f, g, h \in \mathbb{Z}[x]$, monici, t.c.

$$f \equiv gh \ (p)$$

$$(g, h) \equiv 1 \ (p)$$

Allora esistono unici $g_1, h_1 \in \mathbb{Z}[x]$ monici t.c.

1. $f \equiv g_1 \cdot h_1 \ (p^2)$
2. $(g_1, h_1) \equiv 1 \ (p^2)$
3. $g_1 \equiv g \ (p)$ e $h_1 \equiv h \ (p)$.

<u>Traccia dim.</u> Scriviamo $g_1 = g + pG$ e $h_1 = h + pH$ con $\deg G < \deg g_1$ e $\deg H < \deg h_1$. Consideriamo

$$f \equiv gh + Fp \equiv g_1 \cdot h_1 \equiv \qquad (\deg F < \deg f)$$

$$\equiv (g + pG)(h + pH)$$

$$\equiv gh + p(gH + hG) \ (p^2)$$

Da cui cerchiamo G, H t.c.

$$gH + hG \equiv F \ (p)$$

poiché $(g, h) \equiv 1 \ (p)$ e $\deg F < \deg gh$ esiste una soluzione t.c. $\deg G < \deg \cancel{h}$ e $\deg H < \deg g$

... l'unicità e il fatto che (g_1, h_1) si provano in modo analogo

Applicando di nuovo la costruzione a f, g_1, h_1, p^2 si trova una soluzione mod p^4....

Oss. Se p dispari esistono 2 radici distinte α, β di $f(x) \equiv 0$ (p) e quindi $f(x)$, $(x-\alpha) = g$, $(x-\beta) = h$ soddisfano le ipotesi del lemma

Es. Calcolare il sollevamento di $f(x) \equiv (x-2)(x-3)$ (23) a 23^2.

Oss. Se $p = 2$ i metodi precedenti non possono essere applicati. Se volete ho messo un link per trattare il caso $p = 2$.

Oss. Mettendo insieme i risultati precedenti e applicando il teorema cinese del resto si ottiene un algoritmo per calcolare $x^2 \equiv n$ (m). (quando esistono)