Matteo Papa *xenobyte* 16/10/2015

16	5	3	2	1	1	1	1	1	1
32	8	4	3	2	1	1	1	1	1
64	13	6	4	3	2	1	1	1	1
128	21	9	5	4	3	2	1	1	1
256	34	13	7	5	4	3	2	1	1
512	55	19	10	6	5	4	3	2	1
1024	89	28	14	8	6	5	4	3	2
2048	144	41	19	11	7	6	5	4	3
4096	233	60	26	15	9	7	6	5	4
8192	377	88	36	20	12	8	7	6	5
16384	610	129	50	26	16	10	8	7	6
32768	987	189	69	34	21	13	9	8	7
65536	1597	277	95	45	27	17	11	9	8
131072	2584	406	131	60	34	22	14	10	9
262144	4181	595	181	80	43	28	18	12	10
524288	6765	872	250	106	55	35	23	15	11
1048576	10946	1278	345	140	71	43	29	19	13
2097152	17711	1873	476	185	92	53	36	24	16

Famiglia di successioni additive e relative considerazioni; numeri di Pisot, possibile legame tra Fibonacci e crittografia

Sebbene le successioni sono oggetti matematici molto antichi, ancora oggi si scoprono nuove caratteristiche riguardo ad esse e studi approfonditi possono ancora essere svolti.
Tutti noi conosciamo almeno per nome la Successione di Fibonacci. Tale successione e' costruita calcolando l'*n*-esimo termine come somma dell'*n-1*-esimo più l'*n-2*-esimo. Partendo dalla coppia generatrice (1,1) si ha quindi che i primi termini della Successione di Fibonacci valgono:

F = 1,1,2,3,5,8,13,21,34,55,89....

Generalizzazioni in cui si sommano tutti gli n termini precedenti (Trinacci, Tetranacci, n-acci...) sono già state studiate. Noi invece ci soffermiamo su un'altra famiglia di Successioni generalizzate di Fibonacci dove a sommarsi sono l'ultimo termine insieme all'*(n-i)*-esimo dove i e' il numero di 1 iniziali che generano tali Successioni. Si può dunque avere per

i=2: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10946 ...

i=3: 1, 1, 1, 2, 3, 4, 6, 9, 13, 19, 28, 41, 60, 88, 129, 189, 277, 406, 595, 872, 1278 ...

i=4: 1, 1, 1, 1, 2, 3, 4, 5, 7, 10, 14, 19, 26, 36, 50, 69, 95, 131, 181, 250, 345 ...

i=5: 1, 1, 1, 1, 1, 2, 3, 4, 5, 6, 8, 11, 15, 20, 26, 34, 45, 60, 80, 106, 140 ...

I due casi estremi per i=1 e i-> infinito sono particolari:

il caso i=1 e' particolare nel senso che se l'n-esimo termine è la somma del precedente con se stesso allora i numeri di tale successione altro non sono che le potenze di 2.

i=1: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576 ...

Per nostra comodità ci riferiremo a tali successioni sia considerando tutti gli 1 iniziali, sia considerando solo i numeri dopo tali sequenze di 1.

Se i → +infinito e non si considerano gli infiniti 1 di tale serie allora la Successione è esattamente l'insieme dei numeri naturali N.

Tutti avranno sentito parlare della sezione aurea. E' un numero magnifico che troviamo in natura spessissimo, ad esempio come rapporto tra la distanza delle venatura di una foglia, o la relativa

spirale aurea nelle conchiglie e in tanti altri casi. Tale numero vale 1.6180339887 = φ ... ed è connesso con la Successione di Fibonacci perchè il rapporto tra due numeri consecutivi di tale successione approssima proprio la sezione aurea.
E se ci fossero numeri analoghi per le nostre successioni?

Per i due casi estremi i=1 e i → infinito e' facile.
Per i = 1 il rapporto e' 2
per i → infinito sia ha i / i-1 che quindi → 1^+
Tutti gli altri quindi si troveranno in questo intervallo (2;1(

Per Fibonacci abbiamo già nominato la sezione aurea quindi $r_{i=2}$ (rapporto) = 1.618 … per gli altri valori invece:

$r_{i=3}$ = 1.4656 …
$r_{i=4}$ = 1.3802 ...
$r_{i=5}$ = 1.3247 …
$r_{i=6}$ = 1.2851 ...
$r_{i=7}$ = 1.2554 …
$r_{i=8}$ = 1.2320 …
$r_{i=9}$ = 1.2131 ...
...

Partiamo da alcune proprietà della sezione aurea per capire se almeno alcune di queste infinite altre costanti le hanno:

Tra le proprietà interessanti della sezione aurea citiamo le seguenti:

E' un numero di Pisot. *
E' la soluzione reale dell'equazione x^2-x-1=0
E' esprimibile come radice di (uno più radice di (uno più radice di …))

*Cosa è un numero di Pisot?

Un numero di Pisot è un numero algebrico *a* tale che e' un numero algebrico soluzione di una equazione a coefficienti interi e deve inoltre valere che i coniugati di Galois sono in valore assoluto minori di uno. Si definiscono coniugati di Galois tutte le soluzioni del polinomio minimo di un certo numero algebrico dove con polinomio minimo si indica il polinomio monico di grado minore la cui soluzione reale è tale numero algebrico preso in considerazione.

Esistono inoltre i “piccoli” numeri di Pisot e con tale dicitura si indicano tutti quei numeri di Pisot minori della sezione aurea. Se ne sono trovati 38 e il piu' piccolo e' definito “Costante di plastica” e vale 1.3247 …

ma non lo abbiamo già visto questo numero? E' proprio la costante che si ottiene per i=4!
Vediamo altri numeri di Pisot, piccoli ancora. Il secondo piu' piccolo e' 1.3802 … anch'esso rapporto di una nostra funzione!

Ci si chiede come si puo' verificare se altre costanti sono numeri di Pisot e, magari, trovare un nuovo “piu' piccolo numero di Pisot”
A riguardo vi è una dimostrazione ad opera di Siegel del 1944 raggiungibile a **[1]**
Cosa può tornare utile per tale congettura?
Prima abbiamo enunciato tra le tante proprietà della sezione aurea quella di essere soluzione di $x^2-x-1 = 0$
E inoltre noto che la costante di plastica e' soluzione di
$x^3-x-1 = 0$
tale equazione e' il polinomio minimo di un altra equazione:
$x^5-x^4-1=0$

in generale si capisce facilmente che tutte le costanti trovate come rapporto di due termini successivi della famiglia di successioni

prese in considerazione sono le soluzioni di una famiglia di equazioni tutte della forma

$$x^i-x^{i-1}-1=0$$

dove i e' pari al numero di 1 iniziali

> Congettura: se si dimostra l'irriducibilità di un polinomio del tipo $x^i-x^{i-1}-1$ o si trova il relativo polinomio minimo e si verifica che l'insieme delle soluzioni, esclusa la costante presa in considerazione relativa a tale equazione, contenga solo numeri minori di uno in valore assoluto, allora tale costante e' un numero di Pisot.

Tale congettura e' verificata nei casi in cui i=2,3,4,5 e se fosse vera anche per un i >= 6 allora si troverebbe un numero più piccolo della costante plastica 1.3237...

Equazioni equivalenti

E' possibile trovare tante altre equazioni la cui soluzione reale rimane una delle costanti scelte a partire dall'equazione di forma $x^i-x^{i-1}-1=0$

il metodo e' iterabile ed e' il seguente:

si fissa k = grado dell'equazione di partenza nella forma $x^i-x^{i-1}-1=0$ ovvero k = i
si incrementa di 1 il grado dell'equazione sostituendo a x^i il monomio $x^{i+1} = x^j$
si aggiunge il monomio $-x^b$ dove b e' la differenza tra il nuovo grado e quello di partenza, cioè vale b = j-k

esempio:

$x^8-x^7-1=0$ ($k=8=x^i$)
$x^9-x^7-x-1=0$
$x^{10}-x^7-x^2-x-1=0$
…
$x^{13}-x^7-x^5-x^4-x^3-x^2-x-1=0$
…

hanno tutte la costante 1.2320 … come soluzione reale.

Ovviamente si può passare da una equazione all'altra senza incrementare ogni volta di un solo grado l'equazione ma bisogna ricordare di aggiungere tanti monomi quanta la differenza tra il nuovo grado ed il vecchio (e il grado maggiore di questi monomi e' proprio tale differenza).

$x^{10}-x^9-1=0$ (costante/soluzione associata: 1,1975)
$x^{13}-x^9-x^3-x^2-x-1=0$

Ritornando alla dimostrazione di Siegel, essa si basa sulle seguenti considerazioni:

Sia S l'insieme dei numeri di Pisot
Sia θ un intero algebrico e si assuma che tutti i suoi coniugati escluso θ siano in valor assoluto minore di 1
Data una dimostrazione di Salem che prova come $\theta = 1$ sia un punto isolato in S, tale asserzione implica che esista un altro $\theta > 1$ anch'esso isolato.

Un punto isolato P è un punto che non ne ha altri “vicini”, ovvero

esiste un ε scelto tale che l'intervallo (P+ε ; P-ε) non contiene altri punti. E questo e' verificato per le nostre costanti, poiché ε possiamo sceglierlo arbitrariamente e basta che sia ε minore della differenza di due costanti successive.

Ritengo che nella dimostrazione di Siegel vi sia una mancanza. Ha utilizzato alcune funzioni generatrici le cui soluzioni sono numeri di Pisot ma non si e' accorto che alcune di queste equazioni avevano la proprietà di essere del tipo $x^i-x^{i-1}-1=0$. Inoltre Siegel ha identificato il numero di plastica come il più piccolo perchè è il minore che ha calcolato utilizzando delle equazioni con la particolarità che più il grado aumentava più la soluzione reale si avvicinava al punto di accumulazione 1,618 … . Invece le costanti che abbiamo trovato noi le abbiamo calcolate utilizzando delle equazioni che al crescere del grado restituiscono una soluzione reale sempre più vicina a 1.

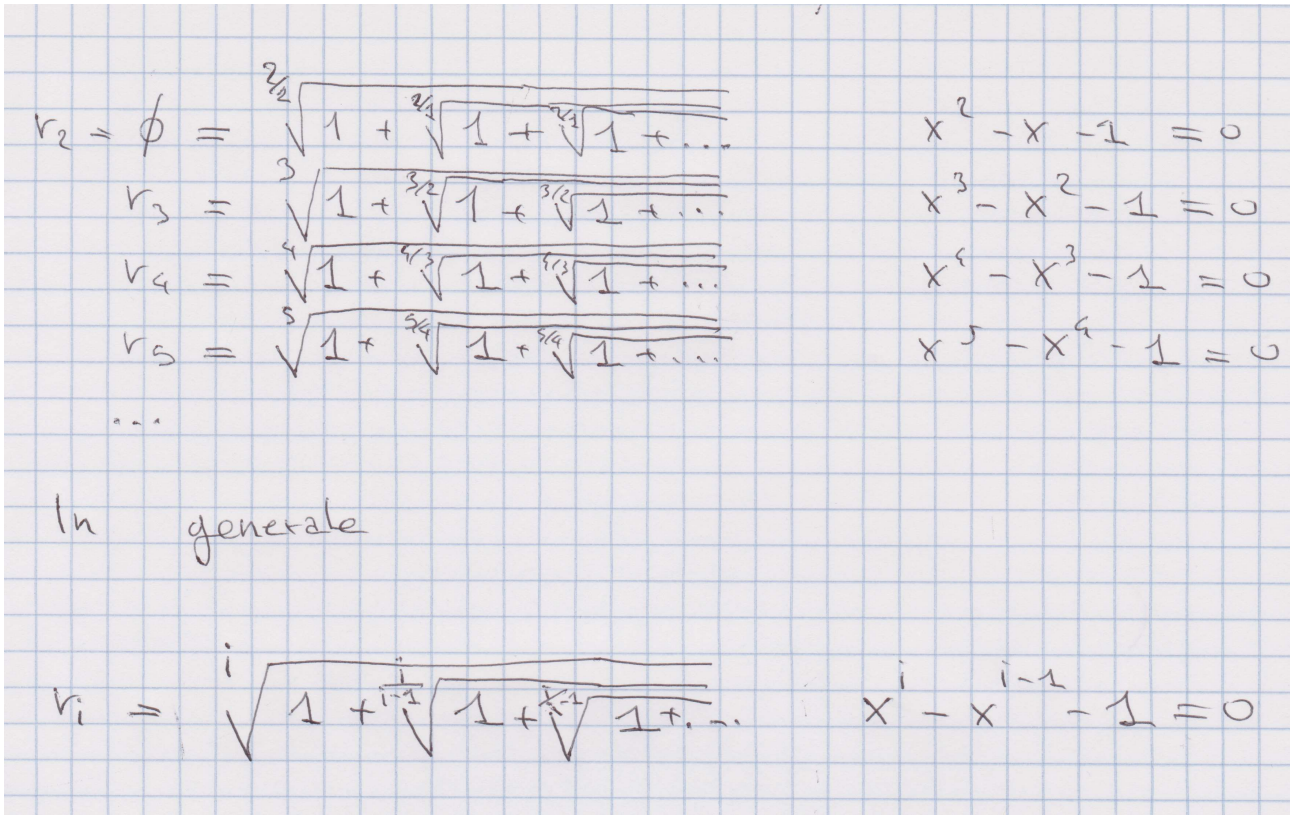
Per comodità potremmo chiamare tali numeri, che siano di Pisot o meno (visto che sebbene abbiano in comune praticamente tutte le proprietà di tali numeri, ancora bisogna verificare l'irriducibilità delle equazioni associate) numeri “di legno”: mi sembra adeguato come nome dato che si passa dalla costante aurea al numero di plastica e i seguenti, appunto “di legno”.

Rappresentazione delle costanti tramite radici

Un modo per rappresentare il valore della sezione aurea è tramite l'utilizzo delle radici. Si ha che

$$\phi = \sqrt{1 + \sqrt{1 + \sqrt{1 + \cdots}}}$$

In modo analogo si puo' scrivere ogni altra costante allo stesso modo sostituendo al primo indice il numero i, e ogni successivo il rapporto i/i-1, dove i fa riferimento alla formula $x^i-x^{i-1}-1=0$ che genera la costante in questione. Ovvero come nella seguente immagine:



Accenni ad altri utilizzi di tali successioni additive:

- Andamento di una popolazione

Così come Fibonacci scoprì la propria successione per risolvere un problema matematico riguardo la crescita di una popolazione di conigli che iniziano ad essere fertili dal primo mese e si accoppiano ogni successivo, tutte le nostre altre serie generalizzate possono essere utilizzate analogamente per studiare l'andamento di una popolazione di individui che iniziano la fertilità in tempi

differenti (ad esempio l'indiano Narayana utilizzò la successione per i=3 per studiare la popolazione delle mucche nel corso degli anni). [2]

- Rapporti numerici in musica e arte

La sezione aurea e' stata utilizzata sia volontariamente sia non spesso in musica (ad esempio nelle opere di Debussy) e più recentemente altri compositori si sono avvicinati alle serie numeriche additive di cui parliamo in questo paper. [2] Anche arti visive sfruttano certi rapporti perchè appaiono “piacevoli” all'occhio umano. [3]

- Altre serie generate dalle nostre?

Se si inizia dalla coppia (4,8) nella prima serie, si scende di due posti e si guarda nella serie successiva, si trova la coppia (8,13); si scende ancora di due posti e si guarda la serie successiva ancora e si trova la coppia (13,19)...continuando cosi' all'infinito abbiamo trovato un collegamento tra tutte le serie che, a due a due, hanno in comune un numero. Se si mettono insieme tutte le coppie e si eliminano i doppi si ottiene la serie

1, 4, 8, 13, 19, 26, 34, 43, 53, 64, 76, 89, 103, 118, 134, 151, 169, 188, 208, 229, 251, 274, 298, 323, 349, 376, 404, 433, 463, 494 ...

Tale serie e' raggiungibile al link https://oeis.org/A034856 e gode di alcune proprietà che non trattiamo in questa discussione ma era interessante citarne la presenza.

- CRITTOGRAFIA e i numeri di Fibonacci

Recentemente si e' iniziato ad utilizzare le curve ellittiche in

crittografia. A parità di lunghezza della chiave utilizzare tali curve permette di accorciare moltissimo i tempi di generazione delle chiavi e di calcolo degli algoritmi.

Una curva ellittica e' una curva definita da una equazione, detta di *Weierstrass* della forma $y^2 = x^3 + ax + b$

L'insieme delle soluzioni di tale equazioni sono ovviamente tutti i punti che compongono la curva e in crittografia possiamo utilizzare questi punti, ad esempio, per scegliere una chiave pubblica e una chiave privata.
Chiaramente, alcuni punti saranno più adatti di altri: essendoci infiniti punti alcuni saranno razionali e altri irrazionali, ovvero i primi siamo in grado di rappresentarli tramite coordinate razionali.
Definendo una curva ellittica definiamo anche delle operazioni che possiamo svolgere su di esse. Di nostro interesse e' la moltiplicazione di un punto.
Dato P un punto che appartiene alla curva ellittica E, possiamo calcolare 2P trovando l'intersezione tra la tangente alla curva in P e la curva stessa, e scegliendo il punto simmetrico a quello trovato come soluzione del problema. Per trovare un punto come nP basterà iterare il processo n volte.
Nella crittografia ellittica questo viene utilizzato per la scelta delel chiavi. Un utente A in particolare deve:

Scegliere un punto P che appartiene alla curva
Scegliere un intero k
Calcolare P* = kP

P* sara' la chiave pubblica di A mentre k sara' la sua chiave privata.
Tutto ovviamente puo' essere implementato in una aritmetica modulare su un campo F_n o ancora meglio, F_p con p un numero primo.

Approfondendo l'argomento in rete mi sono imbattuto in alcuni altri documenti dove venivano mostrati diversi punti razionali sulle curve ellittiche ([3] e [4] e in particolare [4] perchè l'intuizione degli studenti si avvicina a quello trattato in queste pagine ma in maniera incompleta: parlano di potenze di due e Fibonacci senza accorgersi che di fatto sono due successioni di una grande famiglia di serie)

Conseguenze possibili su un collegamento tra tali punti e i valori delle successioni presentate *potrebbe* avere un impatto sulla crittografia ellittica: due prime ipotesi che si possono fare sono che 1) potrebbe essere possibile restringere i valori da verificare nel caso si volesse eseguire un attacco di forza bruta 2) potrebbe (molto difficilmente ma non si puo' mai sapere!) essere possibile trovare un collegamento diretto tra tali valori, i coefficienti della curva utilizzata e le chiavi per risalire in qualche modo dalla chiave pubblica a quella privata e quindi “rompere” la crittografia ECC.

RIFERIMENTI:

[1] Duke Math. J. Volume 11, Number 3 (1944), 597-602. Algebraic integers whose conjugates lie in the unit circle . Carl Ludwig Siegel Purtroppo è accessibile solo la prima pagina all'indirizzo

https://projecteuclid.org/euclid.dmj/1077472667#ui-tabs-1

[2] Narayana's Cows and Delayed Morphisms
http://kalvos.org/johness1.html

[3] Crittosistemi basati su Curve Ellittiche

http://www.di.unisa.it/professori/ads/corso-security/www/CORSO-0001/ECC/index.htm

[4] Congettura sulle curve ellittiche con punti razionali connessi ai numeri di Fibonacci.

http://nardelli.xoom.it/virgiliowizard/sites/default/files/sp_wizard/docs/Fibonacci%20e%20punti%20razionali%20sulle%20curve%20ellittiche_0.pdf

ORIGINALITA' DELLO STUDIO:

Tale studio personale è iniziato per mia curiosità matematica, i riferimenti che ho trovato sono veramente pochi e mi scuso in anticipo se l'articolo è scritto male, contiene errori (la mia conoscenza matematica non va molto più avanti di quella che mi ha dato il liceo scientifico) o se lo stesso argomento è già stato studiato più nel dettaglio e con conclusioni differenti dalle mie e migliori. In qualsiasi caso commenti o critiche costruttive farebbero piacere e potete scrivermi all'indirizzo *matteopapa93@gmail.com*

RINGRAZIAMENTI:

@Un ringraziamento a Roberto Bindi per la possibilità di pubblicare questo pdf sul suo portale https://aitch.me