Corso di Crittografia A.A. 2017-2018

Note sui test di primalità

Leonardo Tamiano

October 18, 2018

Contents

1 Introduzione ai test di primalità

I numeri primi sono degli strumenti molto importanti nel campo della matematica e, in particolare, nel campo della crittografia. Svariate applicazioni crittografiche, compresi i crittosistemi che vengono utilizzati nel mondo del web per proteggere i nostri dati, necessitano, per funzionare, di numeri primi molto grandi. Sorge dunque il problema di generare in modo sicuro numeri primi molto grandi.

Generare in modo sicuro numeri primi molto grandi è un problema difficile. Per semplificarci la vita noi studieremo un problema correlato al problema della generazione di numeri primi grandi. Il problema che tratteremo è il seguente: dato un numero n, esiste un modo per verificare se questo numero è un numero primo? Una procedura che prende in input un intero $n \in \mathbb{N}$ e che ritorna *True* se n è primo, oppure *False* se n non è primo prende il nome di *test di primalità*. Lo scopo di queste note è quindi analizzare i più semplici test di primalità.

Notiamo subito che un banale test di primalità è la fattorizzazione: dato un intero n, se troviamo una fattorizzazione non banale di n, allora il numero non è primo; altrimenti è primo. Ricordiamo però che il problema della fattorizzazione di un numero intero n è un problema per cui ancora non si conosce una soluzione polinomiale. Dato che a noi interessano test di primalità pratici, ovvero di costo polinomiale, possiamo escludere la fattorizzazione come test di primalità in quanto la quantità di risorse richieste risulta essere troppo elevata.

Il test di primalità che utilizza la fattorizzazione viene detto algoritmo *deterministico*. La parola deterministico nel contesto dell'informatica significa che possiamo immaginare l'esecuzione dell'algoritmo come una sequenza di passi determinati dal particolare input. Ogni volta che azioniamo un algoritmo deterministico con lo stesso input, troveremo la stessa sequenza di passi eseguiti. Dunque il comportamento dell'algoritmo è *pre-determinato* dall'input e dall'algoritmo stesso.

I test di primalità che andremmo a vedere si basano invece su algoritmi *probabilistici*, ovvero algoritmi che nel corso della loro esecuzione effettuano scelte *random*. Questo vuol dire che, a differenza di un algoritmo deterministico, un algoritmo probabilistico non esegue sempre la stessa sequenza di mosse quando riceve lo stesso input. Una particolarità degli algoritmi probabilistici è che non sempre ottengono la risposta esatta. Ad un algoritmo probabilistico è invece associata una probabilità di successo; probabilità che varia in base all'input e all'algoritmo stesso. Molto spesso quando trattiamo di algoritmi probabilistici utilizziamo la frase "un evento X succede con alta probabilità". Senza dare una definizione formale, diciamo che questa frase significa che durante l'esecuzione dell'algoritmo la maggior parte delle volte si verifica l'evento X. Nel contesto dei test di primalità, dire che un test funziona con alta probabilità significa dire che la probabilità che il test ci da una risposta errata è molto, molto bassa.

Chiudiamo questa introduzione notando che tutti i test di primalità presi in considerazione fanno utilizzo di condizioni *necessarie* affinché un intero n sia un primo. Una condizione necessaria, come la parola suggerisce, è una condizione che deve essere rispettata se vogliamo che n sia primo. L'idea alla base di

questi test è quella di verificare se n non rispetta una condizione necessaria alla primalità: in tal caso, possiamo dire con certezza che n non è primo. Invece, se n rispetta la condizione necessaria, *non è detto* che n sia primo. In quest'ultimo caso possiamo limitare la probabilità che n rispetti la condizione necessaria non essendo primo, ottenendo così un test di primalità di tipo probabilistico.

2 Pseudoprimo in base b

La prima condizione necessaria che utilizziamo per definire un test di primalità ci è data dal *Piccolo Teorema di Fermat*, che afferma che, dato p primo, allora

$$\forall a \in \mathbb{Z} : a \not| p : a^{p-1} \equiv 1 \mod p$$

Da questo segue che, se n è un intero per cui esiste un a, coprimo con n e tale che $a^{n-1} \not\equiv 1 \mod n$, allora n è sicuramente composto. Se invece abbiamo che $a^{n-1} \equiv 1 \mod n$, non è detto che n sia primo. Andiamo dunque a caratterizzare questi particolari casi con la definizione di pesudoprimo in base b.

Definizione 2.1. Sia n dispari non primo e sia b un intero tale che $MCD(n, b) = 1$. Allora, se

$$b^{n-1} \equiv 1 \mod n$$

n è detto *pseudoprimo in base b*.

Dunque n è uno pseudoprimo in base b se "si comporta come un primo", per il particolare intero b. Dimostreremo nei prossimi risultati che, se un numero non è primo, allora in molti casi non si può "comportare come un primo". Per abbreviare la notazione scriveremo n pp base b per intendere n è pseudoprimo in base b.

2.1 Quanti pseudoprimi in base b esistono?

Proposizione 2.1. Esistono infiniti numeri pseudoprimi in base 2.

Proof. Supponiamo che n sia uno pseudoprimo in base 2 e definiamo il numero $m := 2^n - 1$. Dimostriamo adesso che anche m è uno pseudoprimo in base 2.

Vogliamo che $2^{m-1} \equiv 1 \mod m$. Notiamo che se $n = ab$, allora $2^a - 1 \mid 2^n - 1$. Infatti, da una identità dimostrata nella lezione 5 del 22/03/2018 otteniamo la seguente

$$2^n - 1 = (2^a)^b - 1 = (2^a - 1)[(2^a)^{b-1} + (2^a)^{b-2} + ... + (2^a) + 1]$$

Sappiamo poi che $2^{n-1} \equiv 1 \mod n$, ovvero che $\exists k \in \mathbb{Z} : \quad 2^{n-1} - 1 = kn$. Sostituendo otteniamo

$$2^{m-1} = 2^{(2^n-1)-1} = 2^{2^n-2} = 2^{2(2^{n-1}-1)} = 2^{2kn}$$

dunque $2^{m-1} - 1 = 2^{2kn} - 1$. Questo poi implica che

$$m = 2^n - 1 \mid 2^{2kn} - 1 = 2^{m-1} - 1$$

ovvero che

$$2^{m-1} \equiv 1 \mod m$$

Per completare la dimostrazione basta far vedere che esiste uno pp in base b. La scelta di $n := 341$ funziona. □

2.2 Proprietà dei pseudoprimi in base b

Proposizione 2.2. Sia n dispari e non primo, allora valgono le seguenti proprietà.

1. n pp base $b \implies ord_{\mathbb{Z}_n^*}(b) \mid n-1$.
2. n pp base $b_1, b_2 \implies n$ pp base $b_1 b_2 \mod n$ e base $b_1 b_2^{-1} \mod n$.
3. n non pp base $b \implies n$ non pp base $b' \in \mathbb{Z}_n^*$ per almeno la metà dei b'.

Proof. 1. Segue dalla teoria dei gruppi.

2. Infatti,
$$(b_1 b_2)^{n-1} \equiv_n b_1^{n-1} b_2^{n-1} \equiv_n 1 \cdot 1 \equiv_n 1$$
$$(b_1 b_2^{-1})^{n-1} \equiv_n b_1^{n-1} (b_2^{n-1})^{-1} \equiv_n 1 \cdot 1^{-1} \equiv_n 1$$

3. Se esiste un tale b allora per ogni $b' \in \mathbb{Z}_n^*$ per cui n è pp base b', si ha che n non è pp in base bb'. Dunque i numeri $b' \in \mathbb{Z}_n^*$ per cui n è pp base in b' non possono essere più della metà. Detto altrimenti, n è pp base b' per al più la metà dei $b' \in \mathbb{Z}_n^*$.

□

2.3 Primo test di primalità

Un possibile pseudocodice è il seguente.

1. n intero dispari preso in input.
2. Si sceglie un intero b tale che $0 < b < n$.
3. Si calcola $\alpha := MCD(b, n)$. Se $\alpha \neq 1$ allora n non è primo e ci si ferma ritornando *False*, altrimenti si continua.
4. Si calcola $\beta := b^{n-1} \mod$. Se $\beta \neq 1$ allora n non è primo e ci si ferma ritornando *False*, altrimenti la probabilità che n è composto è $\leq 1/2$.

L'idea dunque è quella di ripete la procedura riportata per $k \in \mathbb{N}$ volte. Se dopo k volte non ci siamo mai fermati e non abbiamo mai ritornato False, allora, assumendo che esiste almeno un $b \in \mathbb{Z}_n^*$ tale che n non è pp base b, la probabilità che n è composto risulta essere $\leq 1/2^k$. Se invece n è composto e tale che non esiste nessun $b \in \mathbb{Z}_n^*$ per cui n non è pp base b, allora il test di primalità riportato non funziona bene, in quanto l'unica volta che ritorna False con n in input è quando trova un fattore di n, e questo avviene con una bassa probabilità. Questa particolare classe di numeri sarà il tema della prossima sezione.

2.4 Numeri di Carmichael

Abbiamo appena definito un test di primalità e abbiamo dimostrato che, *sotto determinate ipotesi*, il test si "comporta bene", ovvero il test riesce a calcolare con alta probabilità e in modo veloce se n è primo oppure no. Se invece n è un numero composto che non rispetta le suddette ipotesi, allora l'unico modo di capire che l'intero in input n è composto è quello di trovare uno dei suoi fattori tramite il calcolo del MCD, il che non è ottimale in quanto pescare un fattore di n in modo randomico è un evento con una bassa probabilità.

Andiamo adesso a formalizzare la classe dei numeri composti che non rispettano le ipotesi di performance del test di primalità appena definito.

Definizione 2.2. Un intero composto n si dice un *numero di Carmichael* se per ogni b con $0 < b < n$ e $MCD(b, n) = 1$, si ha che

$$b^{n-1} \equiv 1 \mod n$$

Dunque un numero composto n è detto numero di Carmicahel se è uno pseudoprimo in base b per ogni b più piccolo di n e coprimo con n. Per rimuovere possibili confusioni invitiamo di andare a riguardare il terzo risultato della proposizione 2.2. Notiamo infine che dalla definizione segue che i numeri di Carmichael non rispettano le ipotesi del terzo risultato.

A seguire presentiamo un risultato tecnico che verrà utilizzato per dimostrare alcuni risultati che caratterizzano questi numeri di Carmichal.

2.4.1 Lemma: $\mathbb{Z}_{p^2}*$ è un gruppo ciclico

Lemma 2.1. $\mathbb{Z}_{p^2}*$ è un gruppo ciclico

Proof. Sappiamo già che $\mathbb{Z}_p^*$ è un gruppo ciclico. Sia α un generatore di $\mathbb{Z}_p^*$. Dimostreremo ora che, o α è un generatore di $\mathbb{Z}_{p^2}*$, oppure $(p+1)\alpha$ è un generatore di $\mathbb{Z}_{p^2}^*$.

Dato che α genera $\mathbb{Z}_p^*$ e che $\mathbb{Z}_p^* \subseteq \mathbb{Z}_{p^2}^*$, si ha che l'ordine di α in $\mathbb{Z}_{p^2}^*$ è almeno $p-1$. Dal Teorema di Lagrange sappiamo poi che l'ordine di un elemento di un gruppo divide il numero di elementi del gruppo, detto anche l'ordine del gruppo. Dato che $\mathbb{Z}_{p^2}^*$ ha $\varphi(p^2) = p(p-1)$ elementi, concludiamo che l'ordine di α in $\mathbb{Z}_{p^2}^*$ divide $p(p-1)$. Dunque abbiamo che $ord_{\mathbb{Z}_{p^2}^*}(\alpha) \geq p-1$ e $ord_{\mathbb{Z}_{p^2}^*}(\alpha) \mid p(p-1)$. A seconda del valore di $ord_{\mathbb{Z}_{p^2}^*}(\alpha)$ abbiamo i seguenti due casi.

1. Se $ord_{\mathbb{Z}_{p^2}^*}(\alpha) > p-1$ allora stiamo a posto e α è un generatore di $\mathbb{Z}_{p^2}^*$. Infatti, dato che $ord_{\mathbb{Z}_{p^2}^*}(\alpha)$ non può essere p, in quanto altrimenti si avrebbe che

$$\begin{aligned} ord_{\mathbb{Z}_{p^2}^*}(\alpha) = p &\implies \alpha^p \equiv 1 \mod p^2 \\ &\implies \alpha^p \equiv 1 \mod p \\ &\implies \alpha \equiv 1 \mod p \end{aligned} \tag{1}$$

il che è un assurdo.

Abbiamo dunque un numero, diverso da p e $p-1$, che divide $p(p-1)$. Questo è solo possibile se il numero è proprio $p(p-1)$. Ma allora $ord_{\mathbb{Z}^*_{p^2}}(\alpha) = p(p-1)$ e α genera $\mathbb{Z}^*_{p^2}$.

2. Se invece $ord_{\mathbb{Z}^*_{p^2}}(\alpha) = p-1$, allora abbiamo che $\alpha^{p-1} \equiv 1 \mod p^2$. Considerando $(p+1)\alpha$ troviamo che

$$\begin{aligned}((p+1)\alpha)^{p-1} &\equiv (p+1)^{p-1}\alpha^{p-1} \mod p^2 \\ &\equiv (p+1)^{p-1} \mod p^2 \\ &\equiv 1 + (p-1)p + (\frac{p-1}{2})p^2 + ... \mod p^2 \\ &\equiv 1 - p \mod p^2 \\ &\not\equiv 1 \mod p^2\end{aligned}$$

Dunque l'ordine di $(p+1)\alpha$ in $\mathbb{Z}^*_{p^2}$ non è $p-1$. Notando infine che $(p+1)\alpha$ è un generatore di $\mathbb{Z}^*_p$, in quanto $(p+1)\alpha \equiv \alpha \mod p$, possiamo utilizzare nuovamente il ragionamento fatto in 1. per concludere che $(p+1)\alpha$ genera $\mathbb{Z}^*_{p^2}$.

□

2.4.2 Caratterizzazione dei numeri di Carmichael

Sia n un numero intero composto. Un numero n viene detto *square-free* quando nella sua fattorizzazione in numeri primi non appare nessun primo con una potenza > 1.

Proposizione 2.3.

1. Se n è divisibile da un quadrato diverso da 1, allora n non è di Carmichael.
2. Sia n square free. n è un numero di Carmichael se e solo se $forall p : [p \mid n \implies p-1 \mid n-1$.

Proof.

1. Supponiamo che n sia divisibile da un quadrato diverso da 1. Allora deve esistere un primo p tale che $p^2 \mid n$. Dal lemma precedente, sappiamo che $\mathbb{Z}^*_{p^2}$ è un gruppo ciclico. Sia g un generatore di $\mathbb{Z}^*_{p^2}$ e sia n' il prodotto dei primi che dividono n diversi da p.

   Per costruzione abbiamo che $MCD(n', p) = 1$. Utilizzando il TCR (Teorema Cinese del Resto) sappiamo che esiste una soluzione $b \in \mathbb{Z}^*_n$ del seguente sistema

$$\begin{cases} x \equiv g \mod p^2 \\ x \equiv 1 \mod n' \end{cases} \tag{2}$$

Dimostriamo quindi che n non è pseudoprimo in base b. Infatti, se per assurdo non fosse così, allora avremmo

$$\begin{aligned} b^{n-1} \equiv 1 \mod n &\implies b^{n-1} \equiv 1 \mod p^2 \\ &\implies ord_{\mathbb{Z}^*_{p^2}}(b) \mid n-1 \end{aligned} \tag{3}$$

Ma dal fatto che $b \equiv g \mod p^2$, segue che $ord_{\mathbb{Z}^*_{p^2}}(b) = \varphi(p^2) = p(p-1)$. Troviamo quindi

$$p(p-1) \mid n-1 \implies p \mid n-1 \tag{4}$$

il che è un assurdo in quanto $p \mid n$. Ma allora n non è pseudoprimo in base b e quindi n non è un numero di Carmichael.

2. Dimostriamo prima il contrapositivo del lato $\implies$. Supponiamo che esiste un p primo tale che $p \mid n$ e $p-1 \nmid n-1$. Vogliamo far vedere che n non è di Carmichael.

   Sia g un generatore di $\mathbb{Z}^*_p$. Consideriamo il seguente sistema cinese, che, dal TCR, ha una soluzione $b \in \mathbb{Z}^*_n$.

   $$\begin{cases} x \equiv g \mod p \\ x \equiv 1 \mod n/p \end{cases} \tag{5}$$

   Allora n non è pp in base b. Infatti, se così non fosse, ovver se n è pp in base b, allora

   $$\begin{aligned} b^{n-1} \equiv 1 \mod n &\implies b^{n-1} \equiv 1 \mod p \\ &\implies ord_{\mathbb{Z}_p}(b) \mid n-1 \end{aligned} \tag{6}$$

   Dato che $b \equiv g \mod p$, sappiamo che $ord_{\mathbb{Z}_p}(b) = p-1$. Troviamo quindi un assurdo, in quanto abbiamo assunto che $p-1 \nmid n-1$ e abbiamo trovato che $p-1 | n-1$. Ma allora n non è di Carmichael.

   Viceversa, supponiamo che per ogni p primo si ha che se $p \mid n$, allora $p-1 \mid n-1$. Facciamo vedere che n è di Carmichael. Sia $n \in \mathbb{Z}^*_n$ e sia p un primo che divide n. Allora $n-1 = (p-1)h$, con $h \in \mathbb{Z}$. Ma allora troviamo che

   $$b^{n-1} = \left(b^{(p-1)}\right)^h \equiv 1 \mod p \tag{7}$$

   Dato che n è square free, possiamo scriverlo come $n = p_1 p_2 ... p_h$, con p_i primi distinti. Ma allora

   $$\begin{aligned} \forall i = 1, ..., h : p_i \mid b^{n-1} - 1 &\implies n = p_1 p_2 ... p_h \mid b^{n-1} - 1 \\ &\implies b^{n-1} \equiv 1 \mod n \end{aligned} \tag{8}$$

   e quindi n è pp in base b. Dato che b era un generico elemento di $\mathbb{Z}^*_n$, abbiamo che n è di Carmichael.

□

Proposizione 2.4. Un numero di Carmichael è il prodotto di almeno tre primi distinti.

Proof. Sia n un numero di Carmichael. Per definizione n non può avere un solo fattore primo. Supponiamo per assurdo che $n = PQ$, con P, Q primi e $P < Q$. Dalla precedente proposizione sappiamo che,

$$\begin{aligned} Q \mid n &\implies Q - 1 \mid n - 1 \\ &\implies n - 1 \equiv 0 \mod (Q - 1) \end{aligned} \tag{9}$$

Inoltre,

$$\begin{aligned} n - 1 &= PQ - 1 \\ &= P(Q - 1 + 1) - 1 \\ &\equiv P - 1 \mod (Q - 1) \\ &\not\equiv 0 \mod (Q - 1) \end{aligned} \tag{10}$$

Il che ci porta chiaramente ad un assurdo. □

3 Pseudoprimo di Eulero in base b

Come abbiamo visto, con il concetto di pseudoprimo in base b siamo riusciti a definire un primo test di primalità. Questo test però non risulta essere efficiente per una particolare classe di numeri, i numeri di Carmichael. Andiamo adesso ad introdurre una nuova condizione necessaria alla primalità.

Da una proposizione dimostrata nella sezione dei *residui quadratici* sappiamo che, se p è un numero primo, allora per ogni $b \in \mathbb{Z}$ si ha che

$$\left(\frac{b}{p}\right) \equiv b^{(p-1)/2} \mod p$$

questo fatto ci permette di motivare la seguente definizione

Definizione 3.1 (Pseudoprimo di Eulero in base b)**.** Diciamo che n è uno pseduoprimo di eulero in base b, abbreviato con n ppE in base b se vale la seguente condizione

$$\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} \mod n$$

3.1 n ppE base $b \implies$ n pp base b

Come prima cosa dimostriamo che il concetto di ppE in base b è "più forte" del concetto di pp in base b.

Proposizione 3.1. Sia n un intero composto. Se n è ppE in base b allora n è anche uno pp in base b.

Proof. Dalle ipotesi segue che

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \mod n \implies b^{n-1} \equiv \left(\frac{b}{n}\right)^2 \mod n$$

dato che $\left(\frac{b}{n}\right) = \pm 1$, ne segue che $\left(\frac{b}{n}\right)^2 = 1$, e quindi che $b^{n-1} \equiv 1 \mod n$, ovvero che n è pp in base b. □

3.2 Numeri di Carmichael non esistono per ppE

Adesso invece dimostriamo che, per quanto riguarda il concetto di ppE in base b, non esiste una classe di numeri analoga alla classe dei numeri di Carmichael per quanto riguarda il concetto di pp in base b.

La dimostrazione verrà spezzata in tre parti, ciascuna delle quali fondamentali per ottenere il risultato desiderato.

3.2.1 P1: n dispari non quadrato, allora $\exists b \in \mathbb{Z}_n^*$ t.c. $(\frac{b}{n}) = -1$

Proposizione 3.2. Sia n dispari e non quadrato. Allora esiste un $b < n$ con $MCD(b, n) = 1$ tale che $\left(\frac{b}{n}\right) = -1$.

Proof. Se n è primo, allora abbiamo fatto in quanto sappiamo dal capitolo sui residui quadratici che per metà dei $b \in \mathbb{Z}_n^*$ si ha $\left(\frac{b}{n}\right) = -1$

Sia quindi n composto. Dato che n non è un quadrato, sappiamo che esiste un primo p che divide n e che compare nella fattorizzazione di n con un esponente dispari e.

Scriviamo $n = p^e m$. Per quanto detto prima sappiamo che esiste un $t \in \mathbb{Z}_p^*$ tale che $\left(\frac{t}{p}\right) = -1$. Dato che $MCD(m, p) = 1$, per il TCR (Teorema Cinese dei Resti) sappiamo che esiste una soluzione per il seguente sistema congruenziale.

$$\begin{cases} x \equiv 1 \mod m \\ x \equiv t \mod p \end{cases}$$

Sia b tale soluzione. Allora si ha che $\left(\frac{b}{n}\right) = -1$. Infatti, utilizzando le regole del simbolo di Jacobi troviamo che

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p^e m}\right) = \left(\frac{b}{p^e}\right)\left(\frac{b}{m}\right) = \left(\frac{b}{p}\right)^e \left(\frac{1}{m}\right) = (-1)^e 1 = -1$$

□

3.2.2 P2: n dispari non primo, allora $\exists b \in \mathbb{Z}_n^* : n$ non è ppE in base b

Questo è il risultato più importante in quanto assicura che se n è dispari e non è primo, allora esisterà sempre un b che potrà essere utilizzato per dimostrare la non-primalità di n.

Proposizione 3.3. Sia n dispari non primo, allora esiste sempre un $b \in \mathbb{Z}_n^*$ tale che n non è ppE in base b.

Proof. Per assurdo assumiamo l'opposto di ciò che vogliamo dimostrare. Assumiamo quindi che per ogni $b \in \mathbb{Z}_n^*$ si ha che n è ppE in base b. Dalla proposizione (3.1) segue che per ogni $b \in \mathbb{Z}_n^*$, n è pp in base b, ovvero che n è un numero di Carmichael.

Avendo caratterizzato i numeri di Carmichael sappiamo dunque che n è square free, ovvero che può essere scritto come prodotto di almeno 3 primi distinti, $n = p_1p_2p_3....p_l$, con p_i primi distinti e $l > 2$.

Per ottenere la contraddizione desiderata dimostreremo che per ogni $b \in \mathbb{Z}_n^*$ si ha che $\left(\frac{b}{n}\right) = 1$. Questo risultato, combinato con la proposizione $P1$, ci porterà ad un assurdo.

Per dimostrare quest'ultimo fatto nuovamente procediamo per assurdo. Assumiamo l'opposto di ciò che vogliamo dimostrare, ovvero assumiamo che esiste un certo $b \in \mathbb{Z}_n^*$ tale che $\left(\frac{b}{n}\right) \equiv_n -1$.

Dato che $MCD(n, n/p_1) = 1$, il TCR ci assicura l'esistenza di una soluzione per il seguente sistema congruenziale

$$\begin{cases} x \equiv 1 & \mod p_1 \\ x \equiv b & \mod n/p_1 \end{cases}$$

Sia $a \in \mathbb{Z}_n^*$ tale soluzione. Dimostriamo adesso che $a^{(n-1)/2} \not\equiv_n \pm 1$. Valgono infatti le seguenti

1. Se $a^{(n-1)/2} \equiv_n 1$, allora $a^{(n-1)/2} \equiv_{n/p_1} 1$. Noi però sappiamo che a è equivalente a b modulo n/p_1, e dato che n è ppE in base b otteniamo che

$$a^{(n-1)/2} \equiv_{n/p_1} b^{(n-1)/2} \equiv_{n/p_1} \left(\frac{b}{n}\right) \equiv_{n/p_1} -1$$

   Dunque $a^{(n-1)/2} \not\equiv_n 1$.

2. Se invece $a^{(n-1)/2} \equiv_n -1$, allora $a^{(n-1)/2} \equiv_{p_1} -1$. Ma sappiamo che $a \equiv 1 \mod p_1$, e dunque $a^{(n-1)/2} \equiv_{p_1} 1$, il che non può essere.

Troviamo quindi una contraddizione in quanto n è ppE in base a, e quindi $a^{(n-1)/2} \equiv_n \left(\frac{a}{n}\right) \equiv_n \pm 1$. □

3.2.3 P3: n dispari non primo allora n non è ppE in base b per almeno la metà dei $b \in \mathbb{Z}_n^*$

Proposizione 3.4. Sia n dispari e non primo. ALlora,

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \mod n$$

è falsa per almeno la metà dei $b \in \mathbb{Z}_n^*$.

Proof. Consideriamo il gruppo moltiplicativo $(Z_n^*, \cdot)$. L'insieme formato da $b \in \mathbb{Z}_n^*$ per cui n è ppE forma un sottogruppo di $\mathbb{Z}_n^*$. Se denotiamo tale insieme con il simbolo A infatti abbiamo

1. $\forall b_1, b_2 \in A : b_1 b_2 \in A$
2. $\forall b \in A : b^{-1} \in A$

Dal Teorema di Lagrange sappiamo che l'ordine di un sottogruppo divide sempre l'ordine del gruppo in cui il sottogruppo è contenuto. In simboli

$$ord(A)k = ord(Z_n^*), \quad k \in \mathbb{N}$$

Dalla proposizione $P2$ abbiamo scoperto che $A \neq \mathbb{Z}_n^*$, e quindi che $k \geq 2$, il che equivale a dire che $1/k \leq 1/2$. Ma allora

$$ord(A) = \frac{ord(\mathbb{Z}_n^*)}{k} \leq \frac{ord(\mathbb{Z}_n^*)}{2}$$

Detto altrimenti, A contiene al più la metà dei $b \in \mathbb{Z}_n^*$. Ma allora $\mathbb{Z}_n^* \setminus A$ contiene almeno la metà dei $b \in \mathbb{Z}_n^*$. □

3.3 Secondo test di primalità (Solovay-Strassen)

Siamo adesso pronti a definire un nuovo test di primalità, che è molto simile al primo test definito, con l'unica differenza che in questo caso utilizziamo la condizione presente nella definizione di ppE in base b.

1. n intero dispari preso in input.
2. Si sceglie un intero b tale che $0 < b < n$.
3. Si calcola $\alpha := MCD(b, n)$. Se $\alpha \neq 1$ allora n non è primo e ci si ferma ritornando *False*, altrimenti si continua.
4. Si calcola $b^{(n-1)/2} \mod n$ e $\left(\frac{b}{n}\right)$ e si verifica se sono equivalenti modulo n, ovvero se $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \mod n$. Se non sono equivalenti, allora n non è primo e ci si ferma ritornando *False*, altrimenti, se sono equivalenti, la probabilità che n è composto è $\leq 1/2$.

Notiamo questa volta che il test non si comporta diversamente in base all'input, in quanto non esistono classi di numeri per cui il test si comporta in modo diverso.

4 Pseudoprimo forte in base b

4.1 Relazione tra ppf in base b e ppE in base b

4.2 Terzo test di primalità (Miller-Rabin)

4.3 Analisi test di primalità di Miller-Rabin