Pocklington test

Proposizione. Sia n un intero. Supponiamo che esistano $x \in \mathbb{Z}$ e Q primo tali che

$$\begin{cases} \gcd(x-1, n) = 1 \\ x^Q \equiv 1 \pmod{n}. \end{cases} \quad (1)$$

Allora per ogni divisore primo p di n vale

$$p \equiv 1 \pmod{Q}.$$

Dim.: La prima condizione in (1) implica $\gcd(x-1, p) = 1$, per ogni divisore primo p di n . In particolare,

$$x \not\equiv 1 \pmod{p}, \quad \forall p|n \text{ primo}. \quad (2)$$

La seconda condizione in (1) implica che $x^Q \equiv 1 \pmod{p}$, per ogni divisore primo p di n . Insieme alla (2), questo implica che x è un elemento di ordine Q in $\mathbb{Z}_p^*$. Ne segue che Q divide $\#\mathbb{Z}_p^* = p-1$, e che

$$p \equiv 1 \pmod{Q}, \quad \forall p|n \text{ primo}, \quad (3)$$

come richiesto.

Corollario. Se $Q > \sqrt{n}$, allora n è primo.

Dim.: Dalla (3) segue che per ogni divisore primo p di n vale $p = 1 + kQ$, per un $k \in \mathbb{Z} > 0$. Dunque $p > \sqrt{n}$, per ogni divisore primo p di n . Assurdo, a meno che n non sia primo.

Goldwasser-Kilian test

Teorema (Goldwasser-Kilian). Sia $n \gg 0$ un intero. Supponiamo che esistano una curva ellittica E su $\mathbb{Z}_n$, un punto $P \in E(\mathbb{Z}_n)$ ed un primo Q con la seguente proprietà:

$$Q \cdot P = \infty \quad \text{in } E(\mathbb{Z}_n), \quad (4)$$

ove ∞ indica il punto all'infinito su $E(\mathbb{Z}_n)$. Allora per ogni divisore primo p di n vale $Q \mid \#E(\mathbb{Z}_p)$.

Dim.: La condizione (4) equivale a richiedere che $Q \cdot P = \infty$ su $E(\mathbb{Z}_p)$, per ogni p , divisore primo di n . Dunque l'ordine del punto P è uguale a Q su $E(\mathbb{Z}_p)$, per ogni p , divisore primo di n . Di conseguenza $Q \mid \#E(\mathbb{Z}_p)$, per ogni p , divisore primo di n .

Corollario. Se $Q > (\sqrt[4]{n} + 1)^2$, allora n è primo.

Per il teorema di Hasse, vale la disuguaglianza

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{Z}_p) \leq p + 1 + 2\sqrt{p}. \quad (5)$$

Scriviamo $p + 1 \pm 2\sqrt{p} = (\sqrt{p} \pm 1)^2$. Dalla (5), dall'ipotesi, e dal fatto che $Q \mid \#E(\mathbb{Z}_p)$, per ogni p , divisore primo di n , abbiamo le disuguaglianze

$$(\sqrt{p} + 1)^2 \geq \#E(\mathbb{Z}_p) \geq Q > (\sqrt[4]{n} + 1)^2,$$

da cui

$$\sqrt{p} + 1 > \sqrt[4]{n} + 1 \quad \Leftrightarrow \quad \sqrt{p} > \sqrt[4]{n} \quad \Leftrightarrow \quad p > \sqrt{n},$$

per ogni p , divisore primo di n . Assurdo, a meno che n non sia primo.

Il test di Goldwasser-Kilian.

Sia $n \gg 0$ un intero (pseudoprimo),

sia $E(\mathbb{Z}_n)$ una curva ellittica random su $\mathbb{Z}_n$;

calcoliamo l'ordine della curva $m := \#E(\mathbb{Z}_n)$ (vedi Osservazione 1).

Supponiamo che m si fattorizzi come $m = r \cdot Q$, con Q primo, $Q > (n^{1/4} + 1)^2$;

costruiamo un punto $X_0 = (U_0, V_0)$ su $E(\mathbb{Z}_n)$ (vedi Osservazione 2);

sia $P := \frac{m}{Q} \cdot X_0$.

Calcoliamo $Q \cdot P$ su $E(\mathbb{Z}_n)$:

se $Q \cdot P = \infty$ su $E(\mathbb{Z}_n)$, (se d è il denominatore non-invertibile che si incontra nel calcolo, deve valere $\gcd(d, n) = n$ (vedi Osservazione 3)), allora $Q \cdot P = \infty$ su $E(\mathbb{Z}_p)$ per ogni divisore primo p di n .

Poiché Q è primo, possiamo concludere che $\text{ord}(P) = Q$ su $E(\mathbb{Z}_p)$ e quindi che Q divide $\#E(\mathbb{Z}_p)$, per ogni divisore primo p di n .

Dopodiché Q primo e $Q > (n^{1/4} + 1)^2$, implica n primo.

• La difficoltà sta nel fattorizzare l'ordine della curva $m := \#E(\mathbb{Z}_n)$: in generale m (che ha l'ordine di grandezza di $n \gg 0$) non si riesce a fattorizzare; nel caso in cui non si riesca ad ottenere nemmeno una fattorizzazione parziale di m del tipo $m = r \cdot Q$, con $Q > (n^{1/4} + 1)^2$ primo o pseudoprimo (in quest'ultimo caso si riparte applicando il test a Q , etc...), si cambia curva.

Osservazione 1. Per calcolare $\#E(\mathbb{Z}_n)$ esiste l'algoritmo di Schoof che è deterministico e polinomiale in $\log n$ (n è pseudoprimo, ma lo trattiamo come se fosse primo). Nelle implementazioni odierne, si usa una variante dell'algoritmo di Goldwasser-Kilian dovuta ad Atkin e Morain: invece che prendere una curva ellittica $E(\mathbb{Z}_n)$ random e contarne i punti, si usano curve ellittiche speciali, la cui cardinalità $\#E(\mathbb{Z}_n)$ è data da una "formula".

Osservazione 2. Per costruire un punto X_0 su $E(\mathbb{Z}_n) : Y^2 = X^3 + AX + B$, si parte da U_0 random, si calcola $U_0^3 + AU_0 + B$, e se ne calcola la radice quadrata modulo n , usando l'algoritmo di Shanks-Tonelli (n è pseudoprimo, ma lo trattiamo come se fosse primo).

Osservazione 3. Se fosse $1 < \gcd(d, n) < n$, allora n sarebbe sicuramente composto.