Algoritmo di Koblitz

Algoritmo che permette di mappare un messaggio $m < p$ su una curva ellittica $E_p(a, b)$ dato un parametro h tale che:

$$(m + 1)h < p.$$

KOBLITZ(m, h, a, b, p)

```
1  for i = 0 to h − 1
2        x = mh + i
3        z = (x^3 + ax + b) mod p
4        if z è un residuo quadratico modulo p
5              y = √z mod p
6              return (x, y)
7  error
```

La probabilità di non trovare un residuo quadratico è circa $1/2^h$.

La complessità è polinomiale, visto che l'estrazione della radice *modulo un primo* è facile.

Estrazione del messaggio

$$m = \left\lfloor \frac{x}{h} \right\rfloor,$$

infatti:

$$\left\lfloor \frac{x}{h} \right\rfloor = \left\lfloor \frac{mh + i}{h} \right\rfloor = \left\lfloor m + \frac{i}{h} \right\rfloor \overset{\frac{i}{h}<1}{=} m.$$