Radici quadrate modulo p, con $p > 2$.

Lemma 1. *Sia $n \in \mathbb{Z}$. Sia $p > 2$ un numero primo.*
(a) n è un quadrato modulo p se e solo se $n^{\frac{p-1}{2}} \equiv 1 \bmod p$;
(b) Sia $n \not\equiv 0$ un quadrato modulo p. Allora l'equazione $x^2 \equiv n \bmod p$ ha 2 soluzioni: a e $b = -a$.
(c) Per determinare $\pm\sqrt{n}$ modulo p si usa l'algoritmo di Shanks-Tonelli oppure quello di Cantor-Zassenhaus.

Dim. (a) Il gruppo $\mathbb{Z}_p^*$ è ciclico di ordine $p-1$. Dal Teorema di Lagrange si ha che per ogni $\bar{x} \in \mathbb{Z}_p^*$ vale $\bar{x}^{p-1} \equiv \bar{1} \bmod p$. In particolare, se $\bar{x} = \bar{a}^2$ è un quadrato, vale $\bar{x}^{\frac{p-1}{2}} \equiv \bar{a}^{p-1} \equiv \bar{1} \bmod p$. Viceversa, supponiamo che $\bar{x}^{\frac{p-1}{2}} \equiv 1 \bmod p$. Sia $\bar{g}$ una radice primitiva in $\mathbb{Z}_p^*$. Scriviamo $\bar{x} = \bar{g}^\alpha$, per un α opportuno. Dall'ipotesi segue che $\bar{x}^{\frac{p-1}{2}} \equiv (\bar{g}^\alpha)^{\frac{p-1}{2}} \equiv \bar{g}^{\frac{\alpha}{2}p-1} \equiv 1 \bmod p$. Poiché $p-1$ è la più piccola potenza di $\bar{g}$ che vale $\bar{1}$, si ha che $\frac{\alpha}{2}$ è necessariamente intero, α è pari e dunque $\bar{x}$ è un quadrato modulo p.
(b) Poiché il polinomio $x^2 - n$ è monico a coefficienti nel campo finito $\mathbb{Z}_p$, l'equazione $x^2 \equiv n \bmod p$ ha al più 2 soluzioni (vedi Nota sulla radice primitiva). Se ne ha una, certamente ne ha due perché se $a^2 = n$, allora $(-a)^2 = n$. D'altra parte, se n è un quadrato modulo p, allora almeno una radice c'è...
(c) Il criterio (a) ci assicura che $\bar{n}$ ha due radici modulo p. Resta il problema di determinarle esplicitamente, in modo efficiente.

Osservazione. Per $n \equiv 0$, l'equazione $x^2 \equiv n \bmod p$ ha 0 come unica soluzione modulo n.

L'algoritmo di Shanks-Tonelli. Sia $p > 2$ un numero primo e sia $a \in \mathbb{Z}$ un quadrato modulo p, quindi tale che $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.
Come calcolare le soluzioni dell'equazione $x^2 \equiv a \bmod p$?

(1) Se $p \equiv 3 \bmod 4$, allora $\sqrt{a} = \{\pm a^{\frac{p+1}{4}}\}$;
Dim. Osserviamo che $\frac{p+1}{4} \in \mathbb{Z}$ se e solo se $p \equiv 3, 7 \bmod 8$. Sia $x = a^{\frac{p+1}{4}}$. Allora
$$x^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1+2}{2}} = a^{\frac{p-1}{2}} \cdot a = a \bmod p.$$

(2) Se $p \equiv 1 \bmod 4$, per calcolare $\sqrt{a}$ è necessario fare una serie di passi. Scriviamo $p - 1 = 2^s \cdot m$, con m dispari. Sia $z \in \mathbb{Z}_p$ una classe a caso che non è un quadrato. Siano
$$c := z^m, \quad u := a^m, \quad v := a^{\frac{m+1}{2}}, \qquad \bmod p.$$

Calcoliamo $u^{2^{s-2}}$.
Se $u^{2^{s-2}} \not\equiv -1 \bmod p$, allora lasciamo invariati u e v, sostituiamo c con c^2:
$$u = u, \quad v = v, \quad c = c^2.$$
Se $u^{2^{s-2}} \equiv -1 \bmod p$, allora sostituiamo u con uc^2, sostituiamo v con vc, lasciamo invariato c:
$$u = uc^2, \quad v = vc, \quad c = c.$$

Calcoliamo $u^{2^{s-3}}$.
Se $u^{2^{s-3}} \not\equiv -1 \bmod p$, allora
$$u = u, \quad v = v, \quad c = c^2.$$
Se $u^{2^{s-3}} \equiv -1 \bmod p$, allora
$$u = uc^2, \quad v = vc, \quad c = c.$$
E così via calcolando $u^{2^{s-2}}, u^{2^{s-3}}, \ldots, u^{2^2}, u^{2^1}$.
All'ultimo passo,
$$c = c^2, \qquad v = vc = \sqrt{a}.$$

Radici quadrate modulo p^k, con $p > 2$.

Lemma 2. *Sia $n \in \mathbb{Z}$. Sia $p > 2$ un numero primo. Sia $k \in \mathbb{N}$.*
(a) n è un quadrato modulo p^k se e solo se n è un quadrato modulo p;
(b) Sia $n \not\equiv 0$ un quadrato modulo p^k. Allora l'equazione $x^2 \equiv n \bmod p^k$ ha 2 soluzioni: a e $-a$.
(c) Sia $n \not\equiv 0$ un quadrato modulo p^k. Le radici quadrate di n modulo p^k si trovano mediante il Lemma di Hensel a partire dalle radici quadrate di n modulo p^{k-1}, che a loro volta si trovano a partire dalle radici quadrate di n modulo p^{k-2}, etc...

Dim.: (a) Siano $S \subset \mathbb{Z}_{p^k}^*$ e $Q \subset \mathbb{Z}_p^*$ i rispettivi sottogruppi dei quadrati. Poiché $\mathbb{Z}_{p^k}^*$ e $\mathbb{Z}_p^*$ sono ciclici, i sottogruppi S e Q hanno indice 2 in $\mathbb{Z}_{p^k}^*$ e $\mathbb{Z}_p^*$, rispettivamente. Consideriamo l'omomorfismo suriettivo $\phi\colon \mathbb{Z}_{p^k}^* \to \mathbb{Z}_p^*$, $x \mapsto \bar{x} \bmod p$, e l'omomorfismo indotto $\bar{\phi}\colon \mathbb{Z}_{p^k}^*/\phi^{-1}(Q) \to \mathbb{Z}_p^*/Q$. L'omomorfismo $\bar{\phi}$ è chiaramente suriettivo. Inoltre, se $\bar{\phi}(x\phi^{-1}(Q)) \in Q$, allora anche $\phi(x) \in Q$ e $x \in \phi^{-1}(Q)$. Dunque $\bar{\phi}$ è anche iniettivo e perciò un isomorfismo. Ne segue che $\phi^{-1}(Q)$ è un sottogruppo di indice 2 in $\mathbb{Z}_{p^k}^*$. Poiché $\mathbb{Z}_{p^k}^*$ è ciclico (ammette un unico sottogruppo di indice due), $\phi^{-1}(Q)$ necessariamente coincide con S. In altre parole n è un quadrato modulo p^k se e solo se $\bar{n} = \phi(n)$ è un quadrato modulo p.
(b) Osserviamo intanto che $x^2 - 1 \equiv 0 \bmod p^k$ se e solo $p^k \mid (x-1)(x+1)$. Poiché nessun primo $p > 2$ può dividere simultaneamente $x-1$ e $x+1$, si ha che $p^k \mid (x-1)$ oppure $p^k \mid (x+1)$. In altre parole $x^2 - 1 \equiv 0 \bmod p^k$ ha esattamente due radici $\bar{1}$ e $\overline{-1}$. Sia adesso $n \not\equiv 0$ un quadrato modulo p^k e siano α e β due radici quadrate di n, per cui vale $\alpha^2 \equiv n \bmod p^k$ e $\beta^2 \equiv n \bmod p^k$. Allora $(\frac{\alpha}{\beta})^2 \equiv 1 \bmod p^k$ e, per quanto provato sopra, $\alpha \equiv \pm\beta \bmod p^k$.
(c) Applichiamo il Lemma di Hensel al polinomio $f(x) = x^2 - n$, con n quadrato $\bmod p^k$, $k \geq 1$. Uno zero di f modulo p^k è una radice quadrata di n modulo p^k. Il Lemma di Hensel dà un metodo per "sollevarla" ad una radice quadrata di n modulo p^k modulo p^{k+1}. Per $k = 1$, una radice quadrata di n modulo p si calcola con l'algoritmo di Shanks-Tonelli. Applicando ripetutamente il Lemma di Hensel si ottiene una radice quadrata di n modulo p^2, poi modulo p^3 ... e così via fino al p^k desiderato.

Dati un polinomio a coefficienti interi $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ e uno zero semplice $a \in Z(f)$ modulo p^k, $k \geq 1$ (questa condizione è espressa dalle condizioni (*)), il Lemma di Hensel dà un metodo per "sollevarlo" ad uno zero $b \in Z(f)$ modulo p^{k+1}. "Sollevarlo" significa che $\phi(b) = a$, dove ϕ è l'omomorfismo suriettivo $\phi\colon Z_{p^{k+1}} \to Z_{p^k}$. In parole povere, $b \equiv a \bmod p^k$.

Lemma di Hensel. *Sia $f \in \mathbb{Z}[x]$ un polinomio. Sia $a \in \mathbb{Z}$ tale che*

$$\begin{cases} f(a) \equiv 0 \bmod p^k \\ f'(a) \not\equiv 0 \bmod p \end{cases}, \qquad k \geq 1. \tag{$*$}$$

Allora esiste un intero $b \in \mathbb{Z}$, unico modulo p^{k+1}, tale che

$$\begin{cases} b \equiv a \bmod p^k \\ f(b) \equiv 0 \bmod p^{k+1}. \end{cases}$$

L'intero b è dato da

$$b \equiv a - f(a) \cdot f'(a)_p^{-1} \mod p^{k+1}, \tag{$**$}$$

dove $f'(a)_p^{-1}$ indica l'inverso di $f'(a)$ modulo p.

Osservazione. (i) Vale $\gcd(f'(a), p) = 1 \Leftrightarrow \gcd(f'(a), p^k) = 1$, per ogni $k \geq 1$. Dunque $f'(a)$ è invertibile modulo p se e solo se è invertibile modulo p^k, per ogni k.
(ii) Nella formula (**), possiamo usare indifferentemente $f'(a)^{-1} \bmod p^{k+1}$ oppure $f'(a)^{-1} \bmod p$: il b che ene risulta sarà lo stesso modulo p^{k+1}.

Proof. Verifichiamo che $b = a + tp^k$, con $t = -f(a)p^{-k} \cdot f'(a)^{-1}$, modulo p^{k+1} soddisfa tutte le proprietà richieste. È chiaro che $b \equiv a \bmod p^k$. Verifichiamo che $f(b) \equiv 0 \bmod p^{k+1}$:
scriviamo $f(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n = \sum_i c_i x^i$, con $c_n \neq 0$. Abbiamo

$$f(b) \equiv \sum_{i=0}^{n} c_i (a + tp^k)^i \equiv \sum_{i=0}^{n} c_i (a^i + \binom{i}{1} a^{i-1} tp^k + \binom{i}{2} a^{i-2} t^2 p^{k2} + \ldots) \equiv \sum_{i=0}^{n} c_i (a^i + i a^{i-1} tp^k) \equiv$$

$$\equiv \sum_{i=0}^{n} c_i a^i + \sum_{i=0}^{n} c_i (i a^{i-1} tp^k) \equiv f(a) + f'(a) tp^k \quad \bmod p^{k+1}.$$

Adesso vediamo che

$$f(b) \equiv 0 \bmod p^{k+1} \quad \Leftrightarrow \quad f(a) + f'(a) tp^k \equiv 0 \bmod p^{k+1}.$$

Poiché $f(a) = sp^k$, per un intero $s \in \mathbb{Z}$, la congruenza qui sopra è equivalente a

$$f(a)p^{-k} + f'(a)t \equiv 0 \bmod p,$$

da cui si ricava

$$t \equiv -f(a)p^{-k} f'(a)_p^{-1} \bmod p$$

e si ottiene

$$b = a + (-f(a)p^{-k} f'(a)_p^{-1}) p^k = a - f(a) f'(a)_p^{-1} \bmod p^{k+1}.$$

Esempio. Sia $p > 2$ un numero primo e sia n un quadrato modulo p, con $n \not\equiv 0 \bmod p$. In questo caso il polinomio è $f(x) = x^2 - n$. Supponiamo che a sia una radice quadrata di n modulo p, cioè $f(a) = a^2 - n \equiv 0 \bmod p$. La derivata soddisfa $f'(a) = 2a \not\equiv 0 \bmod p$, poiché $a^2 \not\equiv 0 \bmod p$ e p è dispari. Il Lemma di Hensel ci dice che esiste un unico intero $b \equiv a \bmod p$ tale che $f(b) = b^2 - n \equiv 0 \bmod p^2$. In altre parole b è una radice quadrata di n modulo p^2.

Similmente, supponiamo che a sia una radice quadrata di n modulo p^k, cioè $f(a) = a^2 - n \equiv 0 \bmod p^k$. Anche in questo caso, $f'(a) = 2a \not\equiv 0 \bmod p^k$, poiché $a^2 \not\equiv 0 \bmod p^k$ e p è dispari. Il Lemma di Hensel ci dice che esiste un unico intero $b \equiv a \bmod p^k$ tale che $f(b) = b^2 - n \equiv 0 \bmod p^{k+1}$. In altre parole b è una radice quadrata di n modulo p^{k+1}.

Applicazione del Lemma di Hensel al calcolo di una radice quadrata modulo p^k, con $p > 2$ primo. Il calcolo consiste nel sollevare una radice quadrata da $\mathbb{Z}_p$ a $\mathbb{Z}_{p^2}$, e successivamente da $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_{p^3}$ e così via fino a $\mathbb{Z}_{p^k}$.

• *Sia $n \in \mathbb{Z}_p$ un quadrato, $n \not\equiv 0 \mod p$, e sia r_1 una sua radice quadrata modulo p:*

$$r_1^2 \equiv n \mod p.$$

Allora

$$r_2 \equiv r_1 - (r_1^2 - n) \cdot (2r_1)^{-1} \bmod p^2$$

è una radice quadrata di n modulo p^2.

Analogamente, possiamo sollevare una radice quadrata da $\mathbb{Z}_{p^i}$ a $\mathbb{Z}_{p^{i+1}}$:

• *Sia $n \in \mathbb{Z}_p$ un quadrato $n \not\equiv 0 \mod p$, e sia r_i una sua radice quadrata modulo p^i:*

$$r_i^2 \equiv n \mod p^i.$$

Allora

$$r_{i+1} \equiv r_i - (r_i^2 - n) \cdot (2r_i)^{-1} \bmod p^{k+1}$$

è una radice quadrata di n modulo p^{k+1}.

Esempio. Sia $p = 7$. I quadrati in $\mathbb{Z}_7^*$ sono $\{1, 2, 4\}$.
- 32 è un quadrato modulo 49, in quanto è un quadrato modulo 7: infatti $32 \equiv 4 \bmod 7$, che è un quadrato in $\mathbb{Z}_7$;
- le radici quadrate di 32 modulo 7 sono 2 e $-2 \equiv 5$;
- le radici quadrate di 32 modulo 49 sono 9 e $-9 \equiv 40$.

Esempio. Sia $p = 7$. I quadrati in $\mathbb{Z}_7^*$ sono $\{1, 2, 4\}$.
- 2 è un quadrato modulo 7: infatti $2^{\frac{p-1}{2}} = 2^3 \equiv 1 \bmod 7$;
- le radici quadrate di 2 modulo 7 sono $a \equiv 3$ e $b \equiv -3 \equiv 4$;
- 2 è un quadrato modulo 49, in quanto è un quadrato modulo 7;
- Calcoliamo la radice quadrata di 2 modulo 49:

$r_1 = 3$;
$r_2 \equiv r_1 - (r_1^2 - 2)(2r_1)^{-1} \equiv 3 - (3^2 - 2) \cdot 6^{-1} \equiv 3 - 7 \cdot 41 \equiv 10 \mod 49$, (usando: $6^{-1} \equiv 41 \mod 49$).
Conclusione: una radice quadrata di 2 modulo 49 è 10, l'altra è $-10 \equiv 39 \mod 49$.
Prova: $10^2 \equiv 2 \mod 49$, $39^2 \equiv 2 \mod 49$.

Esempio. Sia $p = 11$. Sia $a = 3$.
- $a = 3$ è un quadrato modulo 11: infatti $3^5 \equiv 1 \bmod 11$;
- le radici quadrate di 3 modulo 11 sono: 5 e $-5 \equiv 6 \bmod 11$;
- calcoliamo le radici quadrate di 3 modulo 121:

$r_1 = 5$;
$r_2 \equiv r_1 - (r_1^2 - 2)(2r_1)^{-1} \equiv 5 - (25 - 3) \cdot 10^{-1} \equiv 5 - 22 \cdot 10 \equiv 27 \mod 121$;
$r_2 \equiv r_1 - (r_1^2 - 2)(2r_1)^{-1} \equiv 5 - (25 - 3) \cdot 10^{-1} \equiv 5 - 22 \cdot 109 \equiv 27 \mod 121$,
(nota: $10^{-1} \equiv 10 \mod 11$ e $10^{-1} \equiv 109 \mod 121$.
Conclusione: le radici quadrate di 3 modulo 121 sono 27 e $-27 \equiv 94 \mod 121$.
Prova: $27^2 \equiv 3 \mod 121$ etc...

Una formula per le radici quadrate modulo p^k, con $p > 2$ primo.

Lemma.
(i) Se se $a \equiv b \bmod p^k$ allora $a^p \equiv b^p \bmod p^{(k+1)}$. In particolare, $a \equiv b \bmod p$, allora $a^p \equiv b^p \bmod p^2$.
(ii) Se $a \equiv b \bmod p$, allora $a^{p^{(k-1)}} \equiv b^{p^{(k-1)}} \bmod p^k$.

Dim.: (i) Se $a \equiv b \bmod p^k$, allora $a = b + xp^k$, per $k \in \mathbb{Z}$. Elevando ambo i termini alla p e usando la formula del binomio di Newton, troviamo

$$a^p = (b + xp^k)^p = b^p + \sum_{i=1}^{p} \binom{p}{i} b^{p-i} x^p p^{ki} \equiv b^p \bmod p^{k+1}.$$

(ii) Si ottiene da (i) ragionando induttivamente.

Proposizione. *Siano $p > 2$ un primo, n un quadrato modulo p e $k \in \mathbb{Z}_{\geq 1}$. Sia $\alpha \in \mathbb{Z}$ una radice quadrata di n modulo p (un intero tale che $\alpha^2 \equiv n \bmod p$). Allora una radice quadrata di n modulo p^k è data da*

$$\beta \equiv w \cdot v \bmod p^k,$$

dove

$$w \equiv n^{\frac{p^k - 2p^{k-1} + 1}{2}} \bmod p^k \qquad \text{e} \qquad v \equiv \alpha^{p^{k-1}} \bmod p^k.$$

Dim.: Applicando il lemma precedente a $\alpha^2 \equiv n \bmod p$, otteniamo

$$(\alpha^2)^{p^{(k-1)}} = (\alpha^{p^{(k-1)}})^2 = n^{p^{(k-1)}} \bmod p^k.$$

Per ottenere una radice quadrata di n, invece che di $n^{p^{(k-1)}}$, riscriviamo l'identità precedente come

$$\alpha^{(2p^{(k-1)})} * n^{(1-p^{(k-1)})} = n \bmod p^k.$$

e dunque

$$\beta^2 = n \bmod p^k, \qquad \beta = \alpha^{p^{(k-1)}} * n^{(1-p^{(k-1)})/2}.$$

Ora l'esponente di n è negativo: per renderlo positivo osserviamo che

$$n^{((p^k - p^{(k-1)})/2)} = 1$$

cosí possiamo rimpiazzare l'esponente $(1 - p^{(k-1)})/2$ con $(1 - p^{(k-1)})/2 + (p^k - p^{(k-1)})/2$. Da ciò segue la formula desiderata.

Radici quadrate modulo 2 e modulo 2^k.

Fatto. Sia n un intero dispari, $n \equiv 1 \bmod 8$.
(a) n è un quadrato modulo 2 $\quad\Leftrightarrow\quad$ $n \equiv 1 \bmod 2$, cioè è dispari. In tal caso $1^2 \equiv 1 \bmod 2$.
(b) n è un quadrato modulo 4 $\quad\Leftrightarrow\quad$ $n \equiv 1 \bmod 4$. Le radici quadrate di 1 modulo 4 sono 1 e 3.
(c) n è un quadrato modulo 8 $\quad\Leftrightarrow\quad$ $n \equiv 1 \bmod 8$. Le radici quadrate di 1 modulo 8 sono 1, 3, 5, 7.
(d) n è un quadrato modulo 2^k, con $k > 3$, $\quad\Leftrightarrow\quad$ $n \equiv 1 \bmod 8$. Una variante del Lemma di Hensel permette di esprimere una radice quadrata di n modulo 2^{k+1} in termini di una radice quadrata modulo 2^k.

Osservazione. Dai punti (c) e (d) segue che se n è un quadrato modulo 2^k, con $k \geq 3$, allora ha quattro radici quadrate modulo 2^k. Se a è una di esse, allora le quattro radici sono date da

$$a, \qquad b = -a, \qquad c = (1 + 2^{k-1})a, \qquad d = -(1 + 2^{k-1})a. \tag{$*$}$$

Poiché a è dispari, è facile verificare che le radici a e $c = (1 + 2^{k-1})a$ sono distinte modulo 2^k.
Se $n = 1$ e $k = 3$, dalla (*) ritroviamo le quattro radici di 1 modulo 8, ossia $1,\ -1 \equiv 7,\ 5,\ -5 \equiv 3$.

Osservazione. Il Lemma di Hensel non si può applicare direttamente nel caso $p = 2$, ossia per sollevare radici quadrate di n modulo 2^k a radici quadrate di n modulo 2^{k+1}. Infatti, nel caso $f(x) = x^2 - n$, vale $f'(x) = 2x$ e $\gcd(2x, 2^k) \neq 1$, per ogni x e per ogni k. Di conseguenza $f'(x)$ non è mai invertibile modulo 2^k e la formula

$$b = a - f(a)f'(a)^{-1} \bmod p^{k+1}$$

non ha senso.
Per poter usare il Lemma di Hensel è necessario fare un cambiamento di variabile.

Per ipotesi, $n \equiv 1 \bmod 8$ può essere scritto come $n = 1 + 8a$. In particolare è dispari e una sua radice quadrata modulo 2^k è necessariamente dispari.
Sia dunque $a = 2c + 1$ una radice quadrata di n modulo 2^k:

$$a^2 - n = (2c+1)^2 = 4c^2 + 4c + 1 - n = 4c^2 + 4c - 8a = 4(c^2 + c - 2a) \equiv 0 \bmod 2^k$$

se

$$c^2 + c - 2a \equiv 0 \mod 2^{k-2}.$$

Applicando il Lemma di Hensel al polinomio $g(y) = y^2 + y - 2a$ con derivata $g'(y) = 2y + 1$, abbiamo che

$$d \equiv c - g(c) \cdot g'(c)^{-1} \equiv c - (c^2 + c - 2a)(2c+1)^{-1} \mod 2^{k-1}$$

è uno zero del polinomio $g(y) = y^2 + y - 2a$ modulo 2^{k-1}. Di conseguenza $b = 2d + 1$ è uno zero del polinomio $x^2 - n$ modulo 2^{k+1}.

Esempio. Sia $n = 17$. Calcoliamo le radici quadrate di n modulo 2^5.
Poiché $n \equiv 1 \bmod 8$, si ha che n è un quadrato modulo 2^k per ogni $k \geq 4$. Scriviamo $n - 1 = 8 \cdot 2$; dunque $a = 2$. Applichiamo il Lemma di Hensel al polinomio $g(Y) = Y^2 + Y - 4$ fino a $k = 3$. Le radici del polinomio $g(Y)$ modulo 2 sono $y_1 = 0$ e $y_1 = 1$. Solleviamo $y_1 = 0$ fino ad uno zero di $g(Y)$ modulo $2^3 = 8$.

$y_1 = 0$ radice del polinomio $g(Y)$ modulo 2;
Una radice di $g(Y)$ modulo $2^2 = 4$ è data da
$y_2 \equiv y_1 - g(y_1) \cdot g'(y_1)^{-1} \bmod 4$
$g(y_1) = -4, \quad g'(y_1) = 1;$
$y_2 \equiv -(-4) = 0 \bmod 4$
Prova: $g(y_2) = -4 \equiv 0 \bmod 4$

Una radice di $g(Y)$ modulo $2^3 = 8$ è data da
$y_3 = y_2 - g(y_2) \cdot g'(y_2)^{-1}$
$g(y_2) = -4, \quad g'(y_2) = 1$
$y_3 \equiv 4 \bmod 8$
Prova: $g(y_3) = 24 \equiv 0 \bmod 8$

Conclusione: $x_3 = 2y_3 + 1 \equiv 2 \cdot 4 + 1 \equiv 9$ è una radice del polinomio $X^2 - 17$ modulo $2^5 = 32$.
Prova: $x_3^2 - 17 = 81 - 17 = 64 \equiv 0 \bmod 32$!!

Le altre tre radici si ottengono dalla prima radice $a \equiv 9$:

$$a = 9, \quad b = -9 \equiv 23, \quad c = 9(1+16) \equiv 25, \quad d = -25 \equiv 7 \qquad \bmod 32.$$

Prova: sono tutte distinte modulo 32 e vale $\quad 9^2 \equiv 23^2 \equiv 25^2 \equiv 7^2 \equiv 17 \quad \bmod 32.$