Bon, je t'explique rapidement d'où vient le schéma de récurrence que je t'ai donné et comment on devrait arriver à démontrer qu'il converge bien vite vers ce que l'on veut.

Le schéma est, je rappelle :

$$A_{i+1} = A_i + (V_i P \% A_i)$$

$$V_{i+1} = (2V_i - V_i^2 B_{i+1}) \% A_{i+1}$$

avec $B_{i+1} = P // A_{i+1}$

1_ D'où ça vient ?

C'est en fait un schéma classique de type Newton :

On cherche des A_i, B_i, V_i tels que

$$A_i B_i \simeq P \quad \text{et} \quad B_i V_i \simeq 1 \pmod{A_i}$$

(Le $\simeq$ signifie que la différence entre les deux membres va être de plus en plus petite lorsque i grandit... bon après, il va falloir quantifier correctement tout ça mais, pour le moment, je ne donne que l'idée.)

La formule pour V_{i+1} est alors assez naturelle ; c'est le schéma classique de type Newton pour calculer l'inverse de B modulo A.

En ce qui concerne la première formule, on l'obtient comme suit : on cherche A_{i+1} et B_{i+1} sous la forme

$$A_{i+1} = A_i + \delta A_i \quad ; \quad B_{i+1} = B_i + \delta B_i .$$

En négligeant les termes en $\delta A_i \cdot \delta B_i$, on en vient à chercher δA_i, δB_i vérifiant :

$$A_i \, \delta B_i + B_i \, \delta A_i = P - A_i B_i$$

soit encore, en regardant modulo A_i :

$$B_i \, \delta A_i \equiv P \pmod{A_i}$$

Comme V_i est supposé être (proche d') un inverse de B_i mod A_i, on trouve bien :

$$\delta A_i = (V_i P) \,\%\, A_i$$

et donc la formule annoncée.

2. Pistes pour la démonstration

Mon idée est de montrer par récurrence sur i que $A_{i+1} - A_i$ et $(1 - V_i B_i) \,\%\, A_i$ sont de plus en plus petits. (Tout ça devrait se quantifier par des polygones de Newton... mais je ne l'ai pas écrit encore.)

Voici comment je pense qu'on peut dérouler la récurrence : j'écris, pour commencer, les divisions euclidiennes de P et $V_i P$ par A_i :

$$P = A_i B_i + S_i$$

et $V_i P = A_i Q_i + R_i$

Par définition de A_{i+1}, j'ai donc $A_{i+1} - A_i = R_i$

Il y a maintenant plusieurs étapes:

① De $P = A_i B_i + S_i = A_{i+1} B_{i+1} + S_{i+1}$, je déduis:

$$R_i B_{i+1} = (B_i - B_{i+1}) A_i + (S_i - S_{i+1})$$

et donc $\quad B_i - B_{i+1} = R_i B_{i+1} \;//\; A_i$

et $\quad S_i - S_{i+1} = R_i B_{i+1} \;\%\; A_i$

Ainsi $\quad B_i - B_{i+1}$ et $S_i - S_{i+1}$ sont petits.

② De $V_i P = V_i(A_i B_i + S_i) = A_i Q_i + R_i$, je déduis:

$$(V_i B_i - Q_i) A_i = R_i - V_i S_i \qquad (*)$$

et donc $\quad R_i \equiv V_i S_i \pmod{A_i}$

soit encore $\quad B_i R_i \equiv S_i + (V_i B_i - 1) S_i \pmod{A_i}$

En comparant les degrés, on trouve:

$$S_i = [\underbrace{B_i R_i}_{\text{petit}} + \underbrace{(1 - V_i B_i)}_{\text{petit}} S_i] \;\%\; A_i$$

donc S_i est petit

et S_{i+1} aussi du coup grâce à ①.

③ De la définition de V_{i+1}, on déduit:

$$V_{i+1} - V_i \equiv V_i \cdot (1 - V_i B_{i+1}) \pmod{A_{i+1}}$$

donc $(V_{i+1} - V_i) \;\%\; A_{i+1}$ est, lui aussi, petit.

[en utilisant que $B_{i+1} - B_i$ est petit - cf ①

et $1 - V_i B_i$ est petit - hypothèse de récurrence]

(4) De $$V_i P = A_i Q_i + R_i$$
$$= (A_{i+1} - R_i) Q_i + R_i$$
et $V_{i+1} P = A_{i+1} Q_{i+1} + R_{i+1}$, je déduis :

$$R_{i+1} \equiv (V_{i+1} - V_i) P + (1 - Q_i) R_i \pmod{A_{i+1}}$$
$$\equiv (V_{i+1} - V_i) S_{i+1} + (1 - Q_i) R_i \pmod{A_{i+1}}$$

De plus $$1 - Q_i = (1 - V_i B_i) + (V_i . B_i - Q_i)$$
$$= (1 - V_i B_i) + (R_i - V_i S_i) \,//\, A_i$$
par (*)

Comme $(1 - V_i B_i)$, R_i et S_i sont petits, il en est de même de $(1 - Q_i)$. Revenant à la formule :

$$R_{i+1} = \left[(V_{i+1} - V_i) S_{i+1} + (1 - Q_i) R_i \right] \% A_{i+1}$$

on voit que R_{i+1} est <u>très</u> petit car on multiplie dans chaque terme de la somme un petit par un autre petit.

(5) On a enfin :

$$1 - V_{i+1} B_{i+1} \equiv 1 - 2 V_i B_{i+1} + V_i^2 B_{i+1}^2 \pmod{A_{i+1}}$$
$$\equiv (1 - V_i B_{i+1})^2 \pmod{A_{i+1}}$$
$$\equiv \Big[\underbrace{(1 - V_i B_i)}_{\text{petit}} + V_i \underbrace{(B_i - B_{i+1})}_{\text{petit}} \Big]^2 \pmod{A_{i+1}}$$

donc $1 - V_{i+1} B_{i+1}$ est lui aussi <u>très</u> petit.
Et la récurrence fonctionne ainsi...