① $p_n \cdot q_{n-1} - p_{n-1} \cdot q_n = (-1)^{n-1}$

Proof by induction on n:

n=0/ $p_0 \cdot q_{-1} - p_{-1} \cdot q_0 = a_0 \cdot 0 - 1 \cdot 1 = (-1) = (-1)^{-1} = (-1)^{0-1}$

n ⇒ n+1/ Assume that the property holds for n:

$$p_n \cdot q_{n-1} - p_{n-1} \cdot q_n = (-1)^{n-1}$$

We need to prove that the property holds for n+1:

$$p_{n+1} \cdot q_n - p_n \cdot q_{n+1} = (a_{n+1} \cdot p_n + p_{n-1}) \cdot q_n - p_n (a_{n+1} \cdot q_n + q_{n-1})$$

$$= a_{n+1} \cancel{p_n \cdot q_n} + p_{n-1} \cdot q_n - \cancel{p_n q_n} \cdot a_{n+1} - p_n \cdot q_{n-1}$$

$$= (-1) \cdot (p_n \cdot q_{n-1} - p_{n-1} \cdot q_n)$$

$$= (-1) \cdot (-1)^{n-1} = (-1)^n = (-1)^{n+1-1}$$ //

② Theorem: $x > 0$, $x = \frac{p \cdot a + R}{q \cdot a + s}$ with $a > 1$,

p, q, R, s natural numbers, $p \cdot s - q \cdot R = \pm 1$ and

$q \geq s > 0$

$\Rightarrow x = [b_0; b_1, b_2, \dots]$ with

$$[b_0; b_1, \dots, b_{m+1}] = \frac{p}{q} \quad \text{and}$$

$$[b_0; b_1, \dots, b_{m-1}, b_m] = \frac{R}{s}.$$

Proof:

Assume that

$$\frac{P}{Q} = [a_0; a_1, \ldots, a_n] = \frac{p_n}{q_n}, \text{ with } P \cdot S - R \cdot Q = (-1)^{n-1}$$

Given that $GCD(P, Q) = 1$ (since $P \cdot S - R \cdot Q = \pm 1$)
and $GCD(p_n, q_n) = 1$

$\Rightarrow P = p_n$ and $Q = q_n$

$$\Rightarrow p_n \cdot S - R \cdot q_n = (-1)^{n-1} = p_n \cdot q_{n-1} - p_{n-1} \cdot q_n$$

$$\Rightarrow p_n \cdot (S - q_{n-1}) = q_n (R - p_{n-1})$$

$\therefore q_n \mid (S - q_{n-1})$ since $GCD(p_n, q_n) = 1$

but $q_n = Q \geq S$

$q_{n-1} > 0$

$\therefore S - q_{n-1} < q_n$

$\therefore S - q_{n-1} = 0 \Rightarrow S = q_{n-1}$

$\Rightarrow q_n \cdot (R - p_{n-1}) = 0$

$\Rightarrow R = p_{n-1}$ since $q_n > 0$

$$\therefore x = \frac{p_n \cdot \alpha + p_{n-1}}{q_n \cdot \alpha + q_{n-1}}$$

Given that $\alpha > 1$:

$$x = [a_0; a_1, \dots, a_n, \alpha]$$

$$\alpha = [a_{n+1}; a_{n+2}, \dots]$$

$$\therefore x = [a_0; a_1, \dots, a_{n-1}, a_n, a_{n+1}, \dots]$$

with $$[a_0; a_1, \dots a_{n-1}] = \frac{P_{n-1}}{q_{n-1}} = \frac{R}{S}$$

and $$[a_0; a_1, \dots, a_n] = \frac{P_n}{q_n} = \frac{P}{Q}$$ //

Theorem: $x > 0$ $\left| x - \frac{P}{q} \right| < \frac{1}{2q^2}$

$\Rightarrow$ $x = [a_0; a_1, \dots]$ with $\frac{P}{q} = [a_0; a_1, \dots, a_n]$

Proof: Assume $\frac{P}{q} = [b_0; b_1, \dots, b_n] = \frac{P_n}{q_n}$

if $x = \frac{P_n}{q_n} = \frac{P}{q}$, then the theorem trivially holds,

so assume that $x \neq \frac{P_n}{q_n}$

given that $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$, we have that

$$\frac{p}{q} - x = \frac{\varepsilon \cdot \theta}{q^2} \quad \text{with} \quad \varepsilon = \pm 1, \quad 0 < \theta < \frac{1}{2}$$

W.l.o.g we assume that $(-1)^{n-1} = \varepsilon$

Let $w = \dfrac{p_{n-1} - x \cdot q_{n-1}}{x \cdot q_n - p_n}$

notices that $x \cdot q_n - p_n \neq 0$ since $x \neq \frac{p_n}{q_n}$

$$\Rightarrow w \cdot (x \cdot q_n - p_n) = p_{n-1} - x \cdot q_{n-1}$$

$$w \cdot x \cdot q_n - w \cdot p_n = p_{n-1} - x \cdot q_{n-1}$$

$$x \cdot (w \cdot q_n + q_{n-1}) = w \cdot p_n + p_{n-1}$$

$$\Rightarrow x = \frac{w \cdot p_n + p_{n-1}}{w \cdot q_n + q_{n-1}}$$

given that $\frac{p}{q} - x = \frac{\varepsilon \cdot \theta}{q^2}$

we have that $\frac{\varepsilon \cdot \theta}{q^2} = \frac{p_n}{q_n} - x$

$$\frac{p_n}{q_n} - x = \frac{p_n}{q_n} - \frac{\omega \cdot p_n + p_{n-1}}{\omega \cdot q_n + q_{n-1}}$$

$$= \frac{\omega \cdot p_n \cdot q_n + p_n \cdot q_{n-1} - \omega \cdot p_n \cdot q_n - p_{n-1} \cdot q_n}{q_n \cdot (\omega \cdot q_n + q_{n-1})}$$

$$= \frac{(-1)^{n-1}}{q_n \cdot (\omega \cdot q_n + q_{n-1})} = \frac{\varepsilon}{q_n \cdot (\omega \cdot q_n + q_{n-1})}$$

$$\therefore \frac{\varepsilon \cdot \theta}{q^2} = \frac{\varepsilon \cdot \theta}{q_n^2} = \frac{\varepsilon}{q_n (\omega \cdot q_n + q_{n-1})}$$

$$\therefore \theta = \frac{q_n}{(\omega \cdot q_n + q_{n-1})}$$

$$\therefore \frac{1}{\theta} = \omega + \frac{q_{n-1}}{q_n}$$

$$\therefore \omega = \frac{1}{\theta} - \frac{q_{n-1}}{q_n}$$

given that $0 < \theta < \frac{1}{2} \Rightarrow 2 < \frac{1}{\theta}$

$$0 < q_{n-1} \leq q_n \Rightarrow \frac{q_{n-1}}{q_n} \leq 1$$

$$\therefore \omega > 1.$$

We conclude that:

$$x = \frac{w \cdot p_n + p_{n-1}}{w \cdot q_n + q_{n-1}} > 0$$

with $w > 1$, $p_n, p_{n-1}, q_n, q_{n-1}$ natural numbers, $p_n \cdot q_{n-1} - p_{n-1} \cdot q_n = \pm 1$ and $q_n \geq q_{n-1} > 0$

Thus, we have by previous theorem that:

$x = [a_0; a_1, a_2, \ldots]$ with

$$[a_0; a_1, \ldots, a_{k-1}] = \frac{p_{n-1}}{q_{n-1}}$$

$$[a_0; a_1, \ldots, a_k] = \frac{p_n}{q_n} = \frac{p}{q}$$

//

Note: The theorem also holds if

$x > 0$ $\left| x - \frac{p}{q} \right| \leq \frac{1}{2q^2}$

given that $0 < q_{n-1} < q_n$ //

Wiener's attack to RSA:

Assume that $N = p \cdot q$ with $q < p < 2q$, and $d < \frac{1}{3} \cdot N^{\frac{1}{4}}$.

Given (N, e) such that $e \cdot d \equiv 1 \bmod \phi(N)$, there is an efficient algorithm that computes d.

Proof:

We know that: $e \cdot d - 1 = k \cdot \phi(N)$

Moreover: $q < \sqrt{N}$ since $N = p \cdot q$ and $q < p$

Thus, $p + q < 2q + q = 3\sqrt{N}$

$$\therefore N - \phi(N) = N - (p-1) \cdot (q-1)$$
$$= \cancel{N} - \cancel{N} + p + q - 1$$
$$< p + q < 3\sqrt{N}$$

$$\Rightarrow \left| \frac{e}{N} - \frac{k}{d} \right| = \left| \frac{e \cdot d - k \cdot N}{N \cdot d} \right|$$

$$= \left| \frac{e \cdot d - k \cdot \phi(N) + k \cdot \phi(N) - kN}{N \cdot d} \right|$$

$$= \left| \frac{1 - k(N - \phi(N))}{N \cdot d} \right| < \left| \frac{k(N - \phi(N))}{N \cdot d} \right| < \frac{k \cdot 3 \cdot \sqrt{N}}{N \cdot d}$$

$$= \frac{3 \cdot k}{d \cdot \sqrt{N}}$$

Given that

$$e \cdot d - 1 = k \cdot \phi(N)$$

we have that:

$$k \cdot \phi(N) < e \cdot d$$

Thus, given that $e < \phi(N)$ (by definition of RSA), we conclude that:

$$k < d < \frac{1}{3} N^{\frac{1}{4}}$$

$$\therefore 3k < N^{\frac{1}{4}} \quad \text{and} \quad \frac{1}{N^{\frac{1}{4}}} < \frac{1}{3d}$$

$$\therefore \left| \frac{e}{N} - \frac{k}{d} \right| < \frac{3 \cdot k}{d \cdot N^{\frac{1}{2}}} < \frac{N^{\frac{1}{4}}}{d \cdot N^{\frac{1}{2}}} = \frac{1}{d \cdot N^{\frac{1}{4}}} < \frac{1}{3d^2} < \frac{1}{2d^2}$$

Thus, we have that:

$$\left| \frac{e}{N} - \frac{k}{d} \right| < \frac{1}{2d^2} \quad \text{and} \quad \frac{e}{N} > 0$$

Thus, by previous theorem:

$$\frac{e}{N} = [a_0; a_1, \ldots, a_\ell]$$

and $\frac{k}{d} = [a_0; a_1, \ldots, a_j]$ with $j \leq \ell$

(notice that $GCD(k, d) = 1$ since $e \cdot d - k \cdot \phi(N) = 1$) //