Pell Numbers Modulo a prime $p \equiv 1 \pmod 8$

Tony Reix (Tony.Reix@laposte.net)

2005, 5th of April - v0.3

This paper presents a numerical study of the Pell numbers modulo a prime number p such that: $p \equiv 1 \pmod 8$.

1 Pell numbers

Pell numbers $U_n(2,-1)$ and $V_n(2,-1)$ are defined by the Lucas sequences where $(P,Q) = (2,-1)$:

$$U_n(P,Q) = PU_{n-1} - QU_{n-2}, \text{ with: } U_0(P,Q) = 0 \text{ and: } U_1(P,Q) = 1$$

$$V_n(P,Q) = PV_{n-1} - QV_{n-2}, \text{ with: } V_0(P,Q) = 2 \text{ and: } V_1(P,Q) = P = 2$$

We will use: U_n and V_n rather than: $U_n(2,-1)$ and $V_n(2,-1)$ hereafter.

2 Already known Properties

2.1 General Properties

First, it is well known that:

If p is prime and $p \equiv 1 \pmod 8$ then:

$$p = a^2 + b^2 \text{ , with } (a,b) \text{ unic .}$$

$$p = x^2 + 2y^2 \text{ , with } (x,y) \text{ unic .}$$

2.2 Properties of Pell numbers

It has already been proven that:

If p is prime and $p \equiv 1 \pmod 8$ then:

$$p \mid U_{\frac{p-1}{2}}$$

$$4 \mid y \iff p \mid U_{\frac{p-1}{4}}$$

3 Conjectured Properties

The following conjectures are based on a numerical study of all primes p such that: $p \equiv 1 \pmod 8$ lower than 4,000,000 .

3.1 Definitions

We define:

η_U as the greatest k such that: $p \mid U_{(p-1)/2^k}$.
η_V as the greatest k such that: $p \mid V_{(p-1)/2^k}$.
η_p as the greatest k such that: $2^k \mid p-1$.
η_y as the greatest k such that: $2^k \mid y$.
π as the period of $\big((U_n \bmod p)$ and $(V_n \bmod p)\big)$.

$$U_{n+\pi} \equiv U_n \pmod p \text{ and } V_{n+\pi} \equiv V_n \pmod p$$

η_π as the greatest k such that: $\pi \times 2^k = p-1$.

Since $D = P^2 - 4Q = 8$ and $({}^{\mathrm{D}}/_{\mathrm{p}}) = 1$, it is well known that $\pi \mid p-1$.
But finding the exact value of π is a difficult task.

Note that η_U , η_p , and η_y always exist, though η_V may not exist.
Hereafter, $\eta_p \geq 3$.

3.2 Divisibility Properties

$$REVOIR \;\; \eta_U = 1 \text{ or } 2 \implies \eta_V = \eta_U + 1, \;\; \text{and } \eta_U \neq \eta_p \qquad (D.I)$$

$$\eta_U \geq 3 \implies \eta_y \geq 3 \quad (\text{ meaning: } \; p \mid U_{(p-1)/8} \implies 8 \mid y\ ) \qquad (D.II)$$

$$\nexists\ \eta_V \iff \eta_U = \eta_p \qquad (D.III)$$

$$\nexists\ \eta_V \implies \eta_\pi = \eta_U - 2 \qquad (D.IV)$$

$$\exists\ \eta_V \implies (\eta_\pi = \eta_U \;\text{ or }\; \eta_\pi = \eta_U - 1) \qquad (D.V)$$

$$\eta_U < \eta_p \iff \eta_V = \eta_U + 1 \qquad (D.VI)$$

3.3 Counting Properties

Hereafter, $\sharp(p\ /\ \mathfrak{P})$ is the number of primes p that verify $\mathfrak{P}$ and such that η_p is equal to a fixed value.

$$\sharp(\ p\ /\ \eta_U = 1\ )\ =\ \sharp(\ p\ /\ \eta_U \geq 1\ )$$

$$\sharp(\ p\ /\ \eta_U = k\ )\ =\ 2 \times \sharp(\ p\ /\ \eta_U = k+1\ )\ \text{, for: } k = 1..\eta_p - 2$$

$$\sharp(\ p\ /\ \eta_U = \eta_p\ )\ =\ \sharp(\ p\ /\ \eta_U = 1)/2^{\eta_p - 2}\ =\ \sharp(\ p\ /\ \eta_U = \eta_p - 1\ )$$