Mod $2^{255}-19$ using 22 12-bit pieces

orig 6/7/16

$2^{255} = 2^3 \cdot X^{21}$ $\quad X = 2^{12}$

divide by $(2^3 \cdot X^{21} - 19)$: $\quad m$

(equiv. to $w_{42} \cdot 2^9 \cdot X^{20}$)

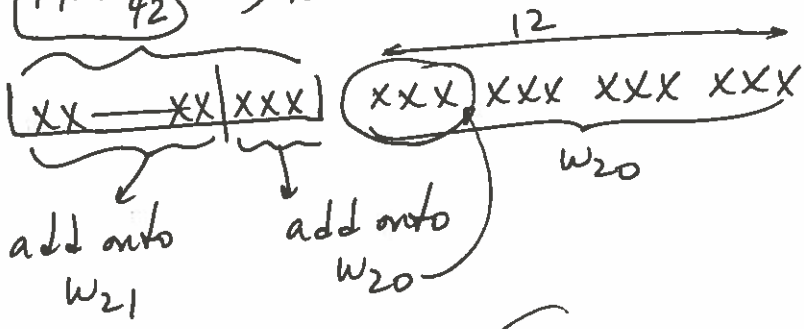
$$2^3 X^{21} - 19 \;\Big)\; w_{42} X^{42} + \cdots + w_{22} X^{22} + \cdots + w_0$$

$w_{42} \cdot 2^{-3} \cdot X^{21}$

$-19 \cdot w_{42} \cdot 2^{-3} \cdot X^{21}$

$$\left(w_{21} + 19 \cdot w_{42} \cdot 2^{-3}\right) X^{21}$$

$(N=22)$ $\quad i=21$



(1) $i = 1 \ldots (N-1)$

$t = 19 \cdot w_{i+N-1}$

$w_i \mathrel{+}= t >> 3$

$w_{i-1} \mathrel{+}= (t \,\&\, 7) << (B-3)$ $\quad$ (B = 9)

$i=1$

$\left(w_1 + 19 \cdot w_{22} \cdot 2^{-3}\right) X$

$i=1, \quad i+N-1 = 1+22-1 = 22$

$i=21, \quad i+N-1 = 21+22-1 = 42$

} w index

→ reduce

(2) if $w_{21} > 7$ adjust: $t = w_{N-1} >> 3$, $w_{N-1} \mathrel{-}= (t << 3)$, $w_0 \mathrel{+}= 19 \cdot t$

$\left((2^3 x^{21} - 19) + t\right)$

reduce (fast – stop when no carry)

(3) if $w \geq m$, subtract m — defer until end