7715

Detailed explanations for the handout (1)
entitled "The Quadratic Residue Number system (QRNS)"; (starting on page (9) i)

(pg 11 i)

Theorem 4: Let m be an integer and let its prime decomposition be $m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_L^{e_L}$, $p_1, p_2, \ldots, p_L$ are primes and $e_1, e_2, \ldots, e_L$ are integers. Then $x^2+1=0$ has two distinct roots in Z_m iff $p_i = 4k_i+1$, $i = 1, 2, \ldots, L$, $k_1, k_2, \ldots, k_L$ are integers.

- Here p_i must be of form $p_i = 4k_i+1$.

Therefore m is also of form $m = 4k+1$. Just see that the product of two forms $4k+1$ is also a form $4k+1$

Proof: $(4k+1)\cdot(4k'+1) = 16\,k\cdot k' + 4k + 4k' + 1 = 4\cdot(4kk' + k + k') + 1 = 4k'' + 1$; $\Rightarrow$ proven.

Detailed explanations for the handout entitled "Multi-Moduli QRNS Systems with Coprime Moduli". ; (starting on page 14 i

Here we only consider moduli forms $2^{n_1}+1$, $2^{n_2}-1$, 2^{n_3}. But $2^{n_3} \neq 4k+1 \Rightarrow$ forms 2^{n_3} are excluded

- Regarding forms $2^{n_2}-1$, let

$$2^{n_2}-1 = 4k+1 \Rightarrow 4k = 2^{n_2}-2 \Rightarrow$$

$$\Rightarrow k = \frac{2^{n_2}-2}{4} = 2^{n_2-2} - \frac{1}{2} \Rightarrow$$

k is not integer $\Rightarrow$ moduli forms $2^{n_2}-1$ are excluded, because $2^{n_2}-1 \neq 4k+1$ where k = integer.

- Regarding forms $2^{n_1}+1$ with n_1 = odd, these forms belong to set S_1; (see S_d sets on page 2 i).

But all these forms $2^{n_1}+1$, $n_1 =$ odd get divided by the first number in S_1 which is $2^1+1=3$ and $3 =$ prime $\neq 4k+1$.
Therefore moduli forms $2^{n_1}+1$, $n_1 =$ odd are also excluded.

<u>Conclusion</u> : Only moduli forms 2^n+1, $n =$ even are allowed for constructing multimoduli QRNS systems.

<u>Pg 16 i ; top line</u>: why is $\langle 2^{-1} \rangle_{2^n+1} = \langle -2^{n-1} \rangle_{2^n+1}$. Just double check and see that $\langle 2 \times (-2^{n-1}) \rangle_{2^n+1}$

$$= \langle -2^n \rangle_{2^n+1} = 2^n+1-2^n = 1.$$

next page

Page 17 i ; set A where

$A = \{m_1, m_2, m_3\} = \{2^{n-2}+1, 2^n+1, 2^{n+2}+1\}$,
$n = 4k+2$, $k = 1, 2, 3$

we need to prove that m_1, m_2, m_3 are pairwise relatively prime or that they belong to three different S_d sets of page 2 i. But just observe that the moduli of set A are three out of the eight moduli of set P of page 6 i for which set P we proved the above

Page 17 i, set B

$B = \{m^*, m_1, m_2, m_3\} =$

$= \{2^{n-6}+1, 2^{n-2}+1, 2^n+1, 2^{n+2}+1\}$,

$n = 8k+6$, $k = 1, 3, 3, \ldots$

we will again prove that m^*, m_1, m_2, m_3 belong to four different S_d sets of page 2 i

Proof: Here $m_2 = 2^n + 1$. But $n = 8k+6$

$= 4 \times 2k + 4 + 2 = 4 \times (2k+1) + 2$

$= 4k' + 2 \Rightarrow \boxed{m_2 \in S_2}$

- $m_1 = 2^{n-2} + 1$; $n = 8k+6 \Rightarrow n-2 = 8k+4$

$\Rightarrow \boxed{m_1 \in S_3}$

- $m_3 = 2^{n+2} + 1$; $n = 8k+6 \Rightarrow n+2 = 8k+8$

$= 8k' =$ multiple of $8 \Rightarrow m_3 \notin S_1$,

$m_3 \notin S_2$, $m_3 \notin S_3$ but ~~it~~ m_3 belongs to some set S_d where $d \geqslant 4$.

- $m^* = 2^{n-6} + 1$; $n = 8k+6 \Rightarrow n-6 = 8k \Rightarrow$

m^* belongs to some set S_d where $d \geqslant 4$.

We now need to prove that

$m^* = 2^{n-6} + 1$, $m_3 = 2^{n+2} + 1$ belong two two different S_d sets. But for the moduli m^*, m_3, their binary exponent difference is 8 (eight)

Therefore m^*, m_3 can't both belong to S_4 (adjacent exp. difference is 16 for S_4) neither can they both belong to S_5 etc .... So m^*, m_3 belong to two different sets S_d, $S_{d'}$, $d \geq 4$, $d' \geq 4$, $d \neq d'$.

The composite conclusion is that the four moduli of set B belong to four different S_d sets $\Rightarrow$ they are pairwise relatively prime (theorem 1)

Page 18 i, set C:

$$C = \{2^{n-14}+1,\ 2^{n-6}+1,\ 2^{n-2}+1,\ 2^n+1,\ 2^{n+2}+1\},$$

$n = 16k+14$, $k = 1, 2, 3, \ldots$

Again we'll prove that the five moduli of C belong to five different S_d sets.

Take 2^n+1. Here $n = 16k+14 = 4 \times 4k + 3 \times 4 + 2 = 4(4k+3)+2 = 4k'+2 \Rightarrow$ $\Rightarrow 2^n+1 \in S_2$.

- Take $2^{n-2}+1$. Here $n=16k+14 \Rightarrow$
$\Rightarrow n-2=16k+12 = 8\times 2k+8+4 =$
$=8(2k+1)+4 = 8k'+4 \Rightarrow 2^{n-2}+1 \in S_3$
- Take $2^{n-6}+1$. Here $n=16k+14 \Rightarrow n-6$
$=16k+8 \Rightarrow 2^{n-6}+1 \in S_4$
- Take $2^{n-14}+1$. Here $n=16k+14 \Rightarrow$
$\Rightarrow n-14=16k \Rightarrow 2^{n-14}+1$ doesn't belong to any of S_1, S_2, S_3, S_4 but $2^{n-14}+1$ belongs to some S_d, $d \geq 5$.
- Take $2^{n+2}+1$. Here $n=16k+14 \Rightarrow n+2$
$=16k+16 = 16k' \Rightarrow 2^{n+2}+1$ belongs to some S_d, $d \geq 5$.

We now only need to prove that $2^{n-14}+1$ and $2^{n+2}+1$ belong to two different S_d sets

NEXT PAGE $\Rightarrow$

Observe that for the moduli $2^{n-14}+1$ and $2^{n+2}+1$ their binary exponents differ by 16. Thus they can't both belong to S_5 (adjacent exp. diff. is 32) nor they can both belong to S_6 (adjacent exp. diff is 64) ----etc. Therefore, $2^{n-14}+1$, $2^{n+2}+1$ belong to two different sets S_d, $S_{d'}$, $d \geq 5$, $d' \geq 5$, $d \neq d'$.

The composite conclusion is that the five moduli of set C belong to five different S_d sets $\Rightarrow$ they are pairwise relatively prime (theorem 1)

Page 18; set D:

$D = \{2^{n-30}+1,\ 2^{n-14}+1,\ 2^{n-6}+1,\ 2^{n-2}+1,\ 2^{n}+1,\ 2^{n+2}+1\}$, $n = 32k+30$, $k = 1, 3, 3, \ldots$

Here it can easily be shown that

if $n = 32k + 30$, then $n = 4k_1 + 2$, and

therefore $2^n + 1 \in S_2$.

It can also be shown that $n-2$ can

take the form $n-2 = 8k_2 + 4 \Rightarrow$

$2^{n-2} + 1 \in S_3$

It can also be shown that $n-6$ can take the form $n-6 = 16k_3 + 8 \Rightarrow 2^{n-6} + 1 \in S_4$

It can also be shown that $n-14$

can take the form $32k + 16 \Rightarrow$

$2^{n-14} \in S_5$.

Regarding the modulus $2^{n-30} + 1$ we

have $n = 32k + 30 \Rightarrow n - 30 = 32k \Rightarrow$

$2^{n-30} + 1$ belongs to some S_d set

with $d \geqslant 6$.

Also $n+2 = 32k + 32 = 32k' \Rightarrow 2^{n+2} + 1$ belongs to some set S_d with $d \geqslant 6$

But for the moduli $2^{n-30}+1$, $2^{n+2}+1$ (which should belong to sets S_d with $d \geq 6$) their binary exp. difference is 32. Therefore they can't both belong to any S_d set with $d \geq 6$ because in S_6 adjacent exp. difference is 64,

in S_7 " " " " 128

etc ....

As a result, $2^{n-30}+1$, $2^{n+2}+1$ belong to two different sets S_d, $S_{d'}$ with $d \geq 6$, $d' \geq 6$, $d \neq d'$

The composite conclusion is that the six moduli of set D belong to six different S_d sets $\Rightarrow$ they are pairwise relatively prime (theorem 1).