Homework 4

Ex 3.6

#64

Let $f(n) = |\mu(n)|$.

Let $(m,n)=1$, $m,n \in \mathbb{Z}^+$. Then

$$f(mn) = |\mu(mn)|$$
$$= |\mu(m)\,\mu(n)| \quad \text{(since } \mu \text{ is multiplicative)}$$
$$= |\mu(m)|\,|\mu(n)|$$
$$= f(m)\,f(n)$$

& f is multiplicative. So by Thm 3.1,

$$F(n) = \sum_{d|n} f(d) = \sum_{d|n} |\mu(d)|$$

is multiplicative. Let p be prime & $a \in \mathbb{Z}^+$.

Then

$$F(p^a) = \sum_{d|p^a} |\mu(d)|$$
$$= |\mu(1)| + |\mu(p)| + |\mu(p^2)| + \cdots + |\mu(p^a)|$$
$$= |1| + |-1| + 0 + \cdots + 0$$
$$= 2.$$

We have $F(n) = 2^{\omega(n)}$

where $\omega(n)$ = # of distinct prime divisors of n.

Now $F(1) = 1 = 2^0 = 2^{\omega(1)}$ & recall since $n=1$.

Now suppose $n > 1$ & $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is a prime factorization. Then

$$F(n) = F(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k})$$
$$= F(p_1^{a_1}) F(p_2^{a_2}) \cdots F(p_k^{a_k}) \quad \text{(since } F \text{ is multiplicative)}$$

$$= \overbrace{2 \cdot 2 \cdot \cdots 2}^{k \text{ times}} \qquad \text{(by result for } F(p^a)\text{)} \quad (2)$$

$$= 2^k$$

$$= 2^{\omega(n)}.$$

$\therefore$

$$F(n) = \sum_{d|n} |\mu(d)| = 2^{\omega(n)} \quad \text{for all } n \geq 1.$$

#65 First we show

$$\ln n = \sum_{d|n} \Lambda(d).$$

The result is true for $n=1$ since $\ln 1 = 0$.

Suppose $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be a prime factorization of $n > 1$.

$$\ln n = \ln(p_1^{a_1} \cdots p_k^{a_k})$$

$$= a \ln(p_1^{a_1}) + \cdots + \ln(p_k^{a_k})$$

$$= a_1 \ln(p_1) + \cdots + a_k \ln(p_k)$$

$$\sum_{d|p_j^{a_j}} \Lambda(d) = \Lambda(1) + \Lambda(p_j) + \cdots + \Lambda(p_j^{a_j})$$

$$= 0 + \ln(p_j) + \cdots + \ln(p_j)$$

$$= a_j \ln p_j.$$

$\therefore$

$$\ln n = \sum_{j=1}^{k} a_j \ln p_j$$

$$= \sum_{j=1}^{k} \sum_{d|p_j^{a_j}} \Lambda(d) = \sum_{d|n} \Lambda(d)$$

(since $\Lambda(m) = 0$ if $m \neq p^a$)

Here $\ln n = \sum_{d|n} \Lambda(d)$ for all $n \geq 1$.

By Möbius Inversion,

$$\Lambda(n) = \sum_{d|n} \mu(d) \ln\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} \mu(d) (\ln n - \ln d)$$

$$= \ln n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \ln d$$

$$= -\sum_{d|n} (\ln d)\, \mu(d)$$

since $\ln n = 0$ if $n = 1$ &

$\sum_{d|n} \mu(d) = 0$ if $n > 1$.

Thus $\Lambda(n) = -\sum_{d|n} \mu(d) \ln d$.

#66 Let $g(n) = f(n)\mu(n)$ where f is mult.

Let $(m,n)=1$ with $m, n \in \mathbb{Z}^+$. Then

$$g(mn) = f(mn)\mu(mn)$$

$$= f(m)f(n)\mu(m)\mu(n) \quad \text{since } f, \mu \text{ are mult.}$$

$$= f(m)\mu(m)\, f(n)\mu(n)$$

$$= g(m)\, g(n) \quad \&$$

g is multiplicative.

Now assume f is multiplicative & $f(1) \neq 1$.

#68

Suppose $F(n) = \sum_{d|n} f(d)$ $\quad (n \geq 1)$

where f is an arithmetic function & F is multiplicative. Then by Möbius Inversion

$$(*) \quad f(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) \text{ for } n \geq 1$$

We proceed as in the proof of Theorem 3.1.

Suppose m, n are relatively prime positive integers.

$$f(mn) = \sum_{d|mn} \mu(d)\, F\left(\frac{mn}{d}\right)$$

$$= \sum_{d_1|m} \sum_{d_2|n} \mu(d_1 d_2)\, F\left(\frac{mn}{d_1 d_2}\right) \quad \text{(by Ex 8. Sect. 3.1)}$$

$$= \sum_{d_1|m} \sum_{d_2|n} \mu(d_1)\mu(d_2)\, F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right)$$

(since if $d_1 | m$ & $d_2 | n$ then $(d_1, d_2) = 1$ since $(m,n) = 1$ and since both μ & F are multiplicative)

$$= \sum_{d_1|m} \mu(d_1)\, F\left(\frac{m}{d_1}\right) \sum_{d_2|n} \mu(d_2)\, F\left(\frac{n}{d_2}\right)$$

$$= f(m)\, f(n) \quad \text{(again by (*))}$$

Hence f is multiplicative.

#5(a)

x	$x^2 \pmod 7$
± 1	1
± 2	4
± 3	$7 \equiv 2$

x	$x^2 \pmod{11}$
± 1	1
± 2	4
± 3	9
± 4	$16 \equiv 5$
± 5	$25 \equiv 3$

$x^2 \equiv 23 \equiv 2 \pmod 7 \iff x \equiv \pm 3 \pmod 7$

$x^2 \equiv 23 \equiv 1 \pmod{11} \iff x \equiv \pm 1 \pmod{11}$

$x^2 \equiv 23 \pmod{77}$ iff $x^2 \equiv 2 \pmod 7$ & $x^2 \equiv 1 \pmod{11}$

iff $x \equiv \pm 3 \pmod 7$ & $x \equiv \pm 1 \pmod{11}$.

We use CRT to solve

$$(*) \begin{cases} x \equiv b_1 \pmod 7 \\ x \equiv b_2 \pmod{11}. \end{cases}$$

$m_1 = 7$, $m_2 = 11$, $M = 77$

$M_1 = 11$, $M_2 = 7$

$x_1 M_1 \equiv 11 x_1 \equiv 1 \pmod 7$ $\quad 4x_1 \equiv 1 \pmod 7$, $x_1 = 2$.

$x_2 M_2 \equiv 7x_2 \equiv 1 \pmod{11}$, $x_2 = 8$.

Sol to $(*) \iff x \equiv x_1 M_1 b_1 + x_2 M_2 b_2$

$\equiv 2 \cdot 11 \cdot b_1 + 8 \cdot 7 \cdot b_2 \pmod{77}$

$b_1 \equiv \pm 3$, $b_2 = \pm 1$

So $x \equiv 22 b_1 + 56 b_2 \pmod{77}$

$\equiv 122, 10, -10, -122$

$\equiv 45, 10, 67, 32$

$\equiv 10, 32, 45, 67 \pmod{77}$

~~$2n+1 = p$ if $n = \frac{p-1}{2}$.~~

~~It follows that $6S = n(n+1)(2n+1) \equiv 0 \pmod p$ &~~

~~$S \equiv 0 \pmod p$ since $p > 3$ & $(6, p) = 1$.~~

~~$\therefore$ S is divisible by p.~~

7 (b) Let p be an odd prime $p > 5$.

By #6

T = Sum of deg-vacs of the q.n.r. mod p

$$\equiv \sum_{k=1}^{p-1} k^2 - \sum_{k=1}^{\frac{p-1}{2}} k^2$$

q_k = q.r $\pmod p$

$$= \sum_{k=1}^{p-1} k^2 - \sum_{j=1}^{\frac{(p-1)}{2}} j^4$$

$$= \frac{1}{6} p(2p-1)(p-1) - \frac{1}{480} p(p-1)(p+1)(3p^2-7)$$

since $\sum_{j=1}^{n} j^4 = \frac{1}{30} n(2n+1)(n+1)(3n^2+3n-1)$.

$$\equiv -\frac{1}{480} p(p-1)(3p^3+3p^2-67p+73)$$

$\therefore$ $480\,T \equiv 0 \pmod p$

& $T \equiv 0 \pmod p$ since $480 = 2^5 \cdot 3 \cdot 5$

& $(p, 480) = 1$ since $p > 5$.

Hence T is divisible by p.

#8 Let p be an odd prime.

P = product of p.r. mod p

$\equiv 1^2 \cdot 2^2 \cdot \cdots \left[\frac{p-1}{2}\right]^2 \pmod{p}$ (by #6).

$\equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$

$\equiv (-1)^{\frac{1}{2}(p+1)} \pmod{p}$ (by Prob. 47(a) Ch. 2)

So if $p \equiv 1 \pmod 4$, $p = 4k+1$ some $k \in \mathbb{Z}^+$ &

$(-1)^{\frac{1}{2}(p+1)} = (-1)^{2k+1} = -1$ &

$P \equiv -1 \pmod p$.

If $p \equiv 3 \pmod 4$, $p = 4k+3$ for $k \in \mathbb{Z}$, $k \geq 0$ &

$(-1)^{\frac{1}{2}(p+1)} = (-1)^{2k+2} = +1$, &

$P \equiv 1 \pmod p$.

Since any odd $p \equiv 1$ or $3 \pmod 4$ we see that

$P \equiv 1 \pmod p$ iff $p \equiv 3 \pmod 4$.

#10(b) Note $4a(ax^2+bx+c) = 4a^2 + 4abx + 4ac$

$= (2a+b)^2 + (4ac - b^2)$.

$x^2 + x \equiv 3 \pmod{13}$

$\Leftrightarrow 4(x^2+x) \equiv 12 \pmod{13}$ (since $(4,13)=1$)

$\Leftrightarrow (2x+1)^2 - 1 \equiv 12 \pmod{13}$

$\Leftrightarrow (2x+1)^2 \equiv 0 \pmod{13}$

$\Leftrightarrow 2x+1 \equiv 0 \pmod{13}$

$\Leftrightarrow 2x \equiv -1 \equiv 12 \pmod{13} \Leftrightarrow x \equiv 6 \pmod{13}$ (since $(2,13)=1$)

Ex 4.2

(12a) Let $a = 11$, $p = 23$. The $\frac{1}{2}(p-1) = 11$.

We want to calculate $11^{11} \pmod{23}$.

$11^2 = 121 \equiv 6 \pmod{23}$.

$11^4 \equiv 36 \equiv 13 \pmod{23}$.

$11^8 \equiv 13^2 \equiv 169 \equiv 8 \pmod{23}$.

$11^{10} = 11^2 \cdot 11^8 \equiv 6 \cdot 8 \equiv 48 \equiv 2 \pmod{23}$,

$11^{11} \equiv 22 \equiv -1 \pmod{23}$.

By Euler's Criterion,

$$\left(\frac{11}{23}\right) \equiv 11^{11} \equiv -1 \pmod{23},$$

& it follows that $\left(\frac{11}{23}\right) = -1$.

(9)

Ex 4.2

#12(b) Use Euler's Criterion to evaluate $\left(\frac{6}{11}\right)$.

$p = 11$, $a = 6$ & $\frac{p-1}{2} = 5$.

$a^5 = (6)^5 = -6^5$

$6^2 = 36 \equiv 3 \pmod{11}$.

$6^4 \equiv 9 \pmod{11}$

$6^5 \equiv 54 \equiv -1 \pmod{11}$ &

$a^5 = (6)^5 \equiv 1 \pmod{11}$.

$\therefore \left(\frac{-6}{11}\right) \equiv 1 \pmod{11}$.

Since 11 is an odd prime this implies $\left(\frac{-6}{11}\right) = 1$.

#13(b) Use Gauss' Lemma to evaluate $\left(\frac{-5}{11}\right)$.

(-5), $2(-5)$, $3(-5)$, $4(-5)$, $5(-5)$

$= -5, -10, -15, -20, -25$

$= (6), 1, (7), 2, (8) \pmod{11}$

$\frac{p}{2} = 5\frac{1}{2}$

$n = 3$

$\left(\frac{-5}{11}\right) = (-1)^3 = -1$

(17)

(a) Let p be a odd prime, a, b be q.n.r. mod p. Then

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1. \quad \text{So}$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)(-1) = 1.$$

Hence ab is q.r. mod p &
$x^2 \equiv ab \pmod{p}$ is solvable

(b) This statement is false.
Let p, q be distinct odd primes & b be q.n.r of both p, q.
If $x^2 \equiv b \pmod{pq}$ where $x \in \mathbb{Z}$
Then

$$pq \mid (x^2 - b) \quad \& \quad p \mid x^2 - b \quad \&$$

$$x^2 \equiv b \pmod{p}$$

which contradicts b be a q.n.r. mod p.
Hence $x^2 \equiv b \pmod{pq}$ is not solvable
for <u>any</u> q.n.r b of p, q.

(18) Let p be an odd prime, $a, b \in \mathbb{Z}$ and suppose $p \nmid a$ & $p \nmid b$.
We have the following TABLE:

$\left(\frac{a}{p}\right)$	$\left(\frac{b}{p}\right)$	$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
1	1	1
1	−1	−1
−1	1	−1
−1	−1	1

From the TABLE we see that either $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) = 1$ or exactly one of $\left(\frac{a}{p}\right), \left(\frac{b}{p}\right), \left(\frac{ab}{p}\right) = 1$.

So among the congruences
$x^2 \equiv a \pmod p$, $x^2 \equiv b \pmod p$, $x^2 \equiv ab \pmod p$
either all three are solvable or
exactly one is solvable.

#14 (e)

$$\left(\frac{-2}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)$$

$$= (+1)(-1) = -1.$$

since $61 \equiv 1 \pmod 4$ & $61 \equiv 5 \pmod 8$

#16(a) $\left(\frac{-1}{7}\right) = -1$ since $7 \equiv 3 \pmod 4$

So there are no integers n: $n^2 \equiv -1 \pmod 7$

ie there are no positive integers n such that $7 \mid (n^2+1)$.

#17(a) Let p be an odd prime & let a, b be quadratic nonresidues mod p.

Then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)(-1) = +1.$

Hence the congruent congruence $x^2 \equiv ab \pmod p$ has a solution $x \in \mathbb{Z}$.

#20 Let a be a positive integer, p an odd prime & suppose $p \nmid a$.

$$\sum_{j=1}^{p-1} \left(\frac{aj}{p}\right) = \sum_{j=1}^{p-1} \left(\frac{a}{p}\right)\left(\frac{j}{p}\right) = \left(\frac{a}{p}\right) \sum_{j=1}^{p-1} \left(\frac{j}{p}\right).$$

$$\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) = 0 \quad \text{since } \frac{p-1}{2} \text{ of } \left(\frac{j}{p}\right) = +1$$

& $\frac{p-1}{2}$ of $\left(\frac{j}{p}\right) = -1$

$1 \le j \le p-1.$

Hence $\sum_{j=1}^{p-1} \left(\frac{aj}{p}\right) = \left(\frac{a}{p}\right) \cdot 0 = 0.$

#21 For each $1 \le j \le p-1$ let $\bar{j}$ be the multiplicative inverse of $j \pmod p$ so that $1 \le \bar{j} \le p-1$ & $j\bar{j} \equiv 1 \pmod p$.

Now $\left(\frac{1}{p}\right)^2 = 1$ &

$1 = \left(\frac{1}{p}\right) = \left(\frac{1 \cdot 1}{p}\right) = \left(\frac{j}{p}\right)\left(\frac{\bar{j}}{p}\right)$ &

$\left(\frac{\bar{j}}{p}\right) = \left(\frac{\bar{j}}{p}\right)$ since $\left(\frac{j}{p}\right)\left(\frac{\bar{j}}{p}\right) = \pm 1.$

Thus $\sum_{j=1}^{p-2} \left(\frac{j(j+1)}{p}\right) = \sum_{j=1}^{p-2} \left(\frac{j}{p}\right)\left(\frac{j+1}{p}\right)$

$= \sum_{j=1}^{p-2} \left(\frac{\bar{j}}{p}\right)\left(\frac{\bar{j}+1}{p}\right)$ (since $\left(\frac{j}{p}\right) = \left(\frac{\bar{j}}{p}\right)$)

$= \sum_{j=1}^{p-2} \left(\frac{\bar{j}(1+j)}{p}\right)$

$= \sum_{j=1}^{p-2} \left(\frac{\bar{j}+1}{p}\right)$ (since $j\bar{j} \equiv 1 \pmod p$)

$= \sum_{k=2}^{p-1} \left(\frac{k}{p}\right)$ since $\overline{(p-1)} = (p-1)$ & $\bar{1} = 1$ so $2 \le j \le p-2$

and j runs thru the residues $1, 2, \ldots, p-2$

$\bar{j}$ runs thru " " $1, 2, \ldots, p-2$

in some order (Note $i \equiv j \pmod p$ iff $\bar{i} \equiv \bar{j} \pmod p$ since mult. inv. is unique mod p)

Hence $$\sum_{j=1}^{p-2} \left(\frac{j(j+1)}{p}\right) = \left(\sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\right) - \left(\frac{1}{p}\right)$$

$$= 0 - 1 = -1$$

Note The result $$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$$

was proved in #20.

#24

(a) Let $p \geq 7$ be prime, so that $p \geq 11$.

$$\left(\frac{10}{p}\right) = \left(\frac{2 \cdot 5}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right)$$

& $p \nmid 2, 5, 10$. At least one of $2, 5, 10$ must be a q.r. mod p since otherwise $\left(\frac{2}{p}\right), \left(\frac{5}{p}\right), \left(\frac{10}{p}\right) = -1$ & $-1 = (-1)(-1)$ which is impossible.

(b) $$\left(\frac{2}{p}\right)\left(\frac{5}{p}\right)\left(\frac{10}{p}\right) = +1.$$

So it is not possible that exactly two of $2, 5, 10$ are q.r mod p since if they were $(+1)(+1)(-1) = +1$ which is impossible.

#22

Suppose p is prime & $p \equiv 1 \pmod 4$.
Then clearly p is odd.
We know from #20 that

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Let $\frac{p+1}{2} \le j \le p-1$ then $1 \le p-j \le \frac{p-1}{2}$
So

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = \sum_{a=1}^{\frac{1}{2}(p-1)} \left(\frac{a}{p}\right) + \sum_{j=\frac{p+1}{2}}^{p-1} \left(\frac{j}{p}\right)$$

$$= \sum_{a=1}^{\frac{1}{2}(p-1)} \left(\frac{a}{p}\right) + \sum_{j=\lfloor \frac{p+1}{2} \rfloor}^{p-1} \left(\frac{-(p-j)}{p}\right)$$

since each $-(p-j) = j - p \equiv j \pmod p$.

$$= \sum_{a=1}^{\frac{1}{2}(p-1)} \left(\frac{a}{p}\right) + \sum_{a=1}^{\frac{1}{2}(p-1)} \left(\frac{a}{p}\right)$$

[since $\left(\frac{-(p-j)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p-j}{p}\right)$
$= \left(\frac{p-j}{p}\right)$ since $b \equiv 1 \pmod 4$
and as j runs thro $\frac{p+1}{2}, \dots, p-1$
$p-j$ runs thro $1, \dots, \frac{p-1}{2}$]

Therefore $2\sum_{a=1}^{\frac{1}{2}(p-1)} \left(\frac{a}{p}\right) = 0$ & $\sum_{a=1}^{\frac{1}{2}(p-1)} \left(\frac{a}{p}\right) = 0$.

#23

Let p be an odd prime & suppose n is q.r. mod p. Then $p \nmid n$ & $p \nmid d$ for any divisor d of n.

Suppose $d \mid n$ & $d > 0$.
Then $\frac{n}{d} \in \mathbb{Z}$ & $\frac{n}{d} \mid n$.

$$\left(\frac{d}{p}\right)\left(\frac{\frac{n}{d}}{p}\right) = \left(\frac{n}{p}\right) = -1$$

since n is q.n.r. mod p. ∎

$$\left(\frac{\frac{n}{d}}{p}\right) = -\left(\frac{d}{p}\right) \quad (*)$$

By Euler's Crit.

$$\sum_{d|n} d^{\frac{p-1}{2}} \equiv \sum_{d|n} \left(\frac{d}{p}\right) \pmod{p}.$$

But $\sum_{d|n} \left(\frac{d}{p}\right) = \sum_{d|n} \left(\frac{n/d}{p}\right)$ (since as d runs thru divisors of n so does n/d)

$$= -\sum_{d|n} \left(\frac{d}{p}\right) \quad \text{(by (*))}$$

Hence $\sum_{d|n} \left(\frac{d}{p}\right) = 0$ &

$$\sum_{d|n} d^{\frac{p-1}{2}} \equiv 0 \pmod{p}.$$

and j runs thru the residues $1, 2, \ldots, p-2$

j runs thru " " $1, 2, \ldots, p-2$

in some order (Note $i \equiv j \pmod p$ iff $\bar{i} \equiv \bar{j} \pmod p$ since mult. inv. is unique mod p)

Hence $$\sum_{j=1}^{p-2} \left(\frac{j(j+1)}{p}\right) = \left(\sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\right) - \left(\frac{1}{p}\right)$$

$$= 0 - 1 = -1$$

Note The result $$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$$

was proved in #20.

#24

(a) Let $p \geq 7$ be prime, so that $p \geq 11$.

$$\left(\frac{10}{p}\right) = \left(\frac{2 \cdot 5}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right)$$

& $\neq 2, 5, 10$. At least one of $2, 5, 10$ must be a q.r. mod p since otherwise $\left(\frac{2}{p}\right), \left(\frac{5}{p}\right), \left(\frac{10}{p}\right) = -1$ & $-1 = (-1)(-1)$ which is impossible.

(b) $$\left(\frac{2}{p}\right)\left(\frac{5}{p}\right)\left(\frac{10}{p}\right) = +1.$$

So it is not possible that exactly two of $2, 5, 10$ are q.r mod p since if they were $(+1)(+1)(-1) = +1$ which is impossible.

(c) At least one of $a = 2, 5$ or 10 is a q.r. mod p.

CASE 1 $a = 2$ then $1, 2$ are q.r. mod p (since $1^2 = 1$).

CASE 2 $a = 5$ then $4, 5$ are q.r. mod p (since $4 = 2^4$)

CASE 3 $a = 10$ then $9, 10$ are q.r. mod p (since $9 = 3^4$)

In all cases there at least two consecutive q.r. mod p

~~#26 PROVED IN CLASS.~~ #25 See NEXT page

#27 Let p, q be prime numbers with $p \equiv 3 \pmod 4$ & $q = 2p+1$. Then clearly p, q are distinct odd primes.

($\Leftarrow$) Suppose $p = 3$. Then $q = 7$ and $2^3 - 1 = 2^p - 1 = 7$ is a Mersenne prime.

($\Rightarrow$) Suppose $2^p - 1$ is a Mersenne prime.

Suppose by way of quadradiction $t = 2^p - 1$ & $p \neq 3$. We show that $q \mid 2^p - 1$.

Now $p = 4n+3$ for some $n \in \mathbb{Z}$ &

$q = 2p+1 = 2(4n+3)+1 = 8n+7$ &

$q \equiv 1 \pmod 8$. Hence

$$\left(\frac{2}{q}\right) = +1.$$

But by Euler $\left(\frac{2}{q}\right) \equiv 2^{\frac{q-1}{2}} = 2^p \pmod q$

& $2^p \equiv 1 \pmod q$ & $q \mid 2^p - 1$ &

$q = 2^n - 1$ since $2^n - 1$ is prime.

But $2^p = (1+1)^p = 1 + \binom{p}{1} + \cdots + \binom{p}{p-1} + 1$

$> 2 + 2p$ (since $p > 3$)

and $2^r - 1 > 2p+1 = q$ ✗ (Contrad.)
Hence $p = 3$.

#25 Let p be prime with $p \equiv 3 \pmod 4$.
Then p is clearly odd.
By Problem # 29 (Ch. 2 p. 63)
which follows per # 47,

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod p.$$

Let n be the # of p.n.r. mod $p < p/2$
i.e. $n \leq \frac{p-1}{2}$.
Then it follows that

$$\left(\frac{1}{p}\right)\left(\frac{2}{p}\right)\cdots\left(\frac{(p-1)/2}{p}\right) = (-1)^n.$$

since n of the terms in the product will be (-1) & the rest $(+1)$. But

$$\left(\frac{1}{p}\right)\left(\frac{2}{p}\right)\cdots\left(\frac{(p-1)/2}{p}\right) = \left(\frac{\left(\frac{p-1}{2}\right)!}{p}\right) \equiv$$

$$= \begin{cases} 1 & \text{if } \left(\frac{p-1}{2}\right)! \equiv 1 \pmod p \\ -1 & \text{if } \left(\frac{p-1}{2}\right)! \equiv -1 \pmod p \end{cases}$$

since $p \equiv 3 \pmod 4$. So

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^n \pmod p.$$