HOMEWORK 2

Section 2.4

#43 (p.63)

(a) Let p be an odd prime.

Case 1. $p=3$. Then $2(p-3)! = 2\cdot 0! = 2 \equiv -1 \pmod 3$.

Case 2 $p>3$.

By Wilson's Theorem

$$(p-1)! \equiv -1 \pmod p.$$

$(p-1)! = (p-1)(p-2)(p-3)!$

$(p-1)(p-2) \equiv (-1)(-2) \equiv 2 \pmod p$ &

$(p-1)! \equiv 2(p-3)! \equiv -1 \pmod p$.

Result is true in both cases.

(b) 103 is an odd prime so by (a),

$$2(100!) \equiv -1 \equiv 102 \pmod{103}.$$

#46 Let p be an odd prime.

Let $x = 1 + \frac{1}{2} + \cdots \frac{1}{p-1}$.

Let

$$m = (p-1)!\,x = \sum_{j=1}^{p-1} \frac{(p-1)!}{j} \in \mathbb{Z}$$

since $j \mid (p-1)!$ for each $1 \le j \le p-1$.

Consider the integers

(*) $\frac{(p-1)!}{1}, \frac{(p-1)!}{2}, \ldots, \frac{(p-1)!}{p-1}$

Suppose $\frac{(p-1)!}{j} \equiv \frac{(p-1)!}{k} \pmod p$,

where $1 \le j,k \le p-1$. Multiplying by jk we have

$(p-1)!\, k \equiv (p-1)!\, j \pmod p$,

$-k \equiv -j \pmod p$, (by Wilson's Thm)

or $k \equiv j \pmod p$

Hence $k = j$ since $1 \le j, k \le p-1$.

It is clear that $p \nmid \frac{(p-1)!}{j}$ for $1 \le j \le p-1$

since p is prime. So it follows that the nos in (*) are congruent mod p to

(**) $1, 2, \ldots, p-1$

in some order.

Hence $m \equiv 1+2+\cdots+(p-1) \pmod p$.

But $1+\cdots+(p-1) = p\left(\frac{p-1}{2}\right) \equiv 0 \pmod p$

since p is odd & $\left(\frac{p-1}{2}\right) \in \mathbb{Z}$.

Hence $m \equiv 0 \pmod p$.

But

$$x = \frac{m}{(p-1)!},$$

$p \mid m$ & $p \nmid (p-1)!$. Hence numerator of x is divisible by p.

#47 Let p be an odd prime.

(a) By Wilson's Theorem

$(p-1)! \equiv -1 \pmod p$.

$$(p-1)! = 1 \cdot 2 \cdots \left(\tfrac{p-1}{2}\right)\left(\tfrac{p+1}{2}\right)\left(\tfrac{p+3}{2}\right) \cdots (p-1)$$

$$= \left(\tfrac{p-1}{2}\right)!\left(p-\left(\tfrac{p-1}{2}\right)\right)\left(p-\left(\tfrac{p-3}{2}\right)\right)\cdots(p-2)(p-1)$$

$$\equiv \left(\tfrac{p-1}{2}\right)!\left(-\left(\tfrac{p-1}{2}\right)\right)\left(-\left(\tfrac{p-3}{2}\right)\right)\cdots(-2)(-1) \pmod p$$

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

Therefore $(-1)^{\frac{1}{2}(p-1)} \left(\left(\tfrac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod p$,

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

or

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

since $\left((-1)^{\frac{1}{2}(p-1)}\right)^2 = (-1)^{p-1} = 1$ since p is odd.

(b) Suppose $p \equiv 1 \pmod 4$. Then
$p = 4q+1$ some $q \in \mathbb{Z}$,

$\frac{p+1}{2} = 2q+1$ is odd & $(-1)^{\frac{p+1}{2}} = -1$.

Hence by (a)

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

So
$x = \left(\frac{p-1}{2}\right)!$ is a solution of the congruence

$$x^2 \equiv -1 \pmod p$$

(c) Suppose $p \equiv 3 \pmod 4$. Then $p = 4q+3$, $q \in \mathbb{Z}$,
$\frac{p+1}{2} = 2q+2$ is even & $(-1)^{\frac{p+1}{2}} = +1$.

So by (a), $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod p$ &
$x = \left(\frac{p-1}{2}\right)!$ is a solution of the congruence $x^2 \equiv 1 \pmod p$.

#48 Let p be an odd prime.

$$\left(\frac{p-1}{2}\right)! = 1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right)$$

$$(p-1)! = 1 \cdot 3 \cdot 5 \cdots (p-2)$$
$$2 \cdot 4 \cdot 6 \cdots (p-1)$$
$$= 1 \cdot 3 \cdot 5 \cdots (p-2)$$
$$(p-(p-2)) \cdot (p-(p-4)) \cdots (p-(p-(p-1)))$$

$$\equiv 1 \cdot 3 \cdot 5 \cdots (p-2)$$
$$(-(p-2))(-(p-4)) \cdots (-(p-(p-1))) \pmod p$$

$$\equiv (-1)^{\frac{p-1}{2}} (1 \cdot 3 \cdot 5 \cdots (p-2))^2 \pmod p.$$

$(p-1)! \equiv -1 \pmod p$ by Wilson's Thm

So

$$(-1)^{\frac{p-1}{2}} (1 \cdot 3 \cdot 5 \cdots (p-2))^2 \equiv (-1) \pmod p$$

Multiplying both sides by $(-1)^{-\frac{1}{2}(p-1)}$ we find

$$(1 \cdot 3 \cdot 5 \cdots (p-2))^2 \equiv (-1)^{\frac{1}{2}(p+1)} \pmod p$$

since p is odd & $(-1)^{p-1} = +1$.

Section 2.5

#54

(a) $561 = (3)(11)(17)$ is clearly composite since 3, 11, 17 are pairwise relatively prime it suffices to show that

$$2^{561} \equiv 2 \pmod{m}$$

for $m = 3, 11,$ and 17.

$2^2 = 4 \equiv 1 \pmod 3$ so

$2^{561} = \left(2^{2}\right)^{280} 2^1 \equiv 1^{280} \cdot 2 \pmod 3$

$\equiv 2 \pmod 3.$

$2^5 = 32 \equiv -1 \pmod{11}$ since $11 \mid 33.$

So

$2^{561} = (2^5)^{112} 2^1 \equiv (-1)^{112} \cdot 2 \pmod{11}$

$\equiv 2 \pmod{11}.$

$2^4 = 16 \equiv -1 \pmod{17}.$

So

$2^{561} = (2^4)^{140} 2^1 \equiv (-1)^{140} \cdot 2 \pmod{17}$

$\equiv 2 \pmod{17}.$

Therefore $m \mid (2^{561} - 2)$ for $m = 3, 11 \& 17.$

Hence

$561 \mid 2^{561} - 2$ since $561 = 3 \cdot 11 \cdot 17$

& 3, 11, 17 are pairwise rel. prime.

Therefore $2^{561} \equiv 2 \pmod{561}$ &

561 is a pseudoprime.

(b) $645 = (3)(5)(43)$ is clearly composite
First we show $2^{645} \equiv 2 \pmod{m}$ for
$m = 3, 5$ and 43.

$2^2 = 4 \equiv 1 \pmod 3$. So $2^{645} = (2^2)^{322} 2^1$
$\equiv 1^{322} 2 \pmod 3$
$\equiv 2 \pmod 3$.

$2^2 = 4 \equiv -1 \pmod 5$. So
$2^{645} = (2^2)^{322} 2^1 \equiv 2(-1)^{322} \cdot 2 \pmod 5$
$\equiv 2 \pmod 5$.

$2^{42} \equiv 1 \pmod{43}$ by Fermat's Little Thm
since 43 is prime & $43 \nmid 2$.

$645 = 15 \cdot (42 + 1)$
$= (42)(15) + 15$.

So
$2^{645} = (2^{42})^{15} 2^{15} \equiv 1^{15} 2^{15} \pmod{43}$
$\equiv 2^{15} \pmod{43}$.

$2^7 = 128 = 2(43) + 42 \equiv -1 \pmod{43}$.

Hence
$2^{15} = (2^7)^2 \cdot 2^1 \equiv (-1)^2 \cdot 2 \pmod{43}$
$\equiv 2 \pmod{43}$.

So $2^{645} \equiv 2 \pmod{43}$.

Therefore $m \mid 2^{645} - 2$ for $m = 3, 5$ & 43.

$645 \mid 2^{645} - 2$ since
$645 = 3 \cdot 5 \cdot 43$ & $3, 5, 43$ are pairwise
relatively prime. Hence
$2^{645} \equiv 2 \pmod{645}$ &
645 is pseudoprime.

#58 Let a, b be integers not divisible by the prime p.

(a) By the Corollary to Fermat's Little Thm
$a^p \equiv a \pmod p$ & $b^p \equiv b \pmod p$
Have if
$a^p \equiv b^p \pmod p$ then $a \equiv b \pmod p$.

(b) Suppose $a^p \equiv b^p \pmod p$.
Then $a \equiv b \pmod p$ by (a).

$$a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1})$$

$p \mid (a-b)$ since $a \equiv b \pmod p$.

$$a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}$$
$$\equiv a^{p-1} + a^{p-2}\cdot a + \cdots + a \cdot a^{p-2} + a^{p-1} \pmod p$$
(since $a \equiv b \pmod p$.)
$$\equiv p\, a^{p-1} \pmod p$$
$$\equiv 0 \pmod p.$$

& $p \mid (a^{p-1} + \cdots + b^{p-1})$ & have
$p^2 \mid (a^p - b^p)$ &

$$a^p \equiv b^p \pmod{p^2}.$$

#59

Let p, q be distinct primes.

Then $p^{q-1} \equiv 1 \pmod{q}$ by Fermat's Little Thm since q is prime & $q \nmid p$ (because distinct primes).

$q^{p-1} \equiv 0 \pmod{q}$ since $p-1 \geq 1$.

Hence

$$p^{q-1} + q^{p-1} \equiv 1 + 0 \pmod{q}$$
$$\equiv 1 \pmod{q}$$

Similarly we have

$$p^{q-1} + q^{p-1} \equiv 0 + 1 \pmod{p}$$
$$\equiv 1 \pmod{p}.$$

Hence $p \mid (p^{q-1} + q^{p-1} - 1)$ & $q \mid (p^{q-1} + q^{p-1} - 1)$

Since p, q are distinct primes (so $(p, q) = 1$) it follows that

$$pq \mid (p^{q-1} + q^{p-1} - 1) \text{ &}$$

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

#62.

(a) Let m, n be positive integers such that $m \mid n$.
Then $(2^m - 1) \mid (2^n - 1)$
by Problem 9, p. 9.

(b) NOTE: need to assume n is composite in this part.
($\Rightarrow$) Suppose n is odd pseudoprime. Then
$$2^n \equiv 2 \pmod n,$$
& $2 \cdot (2^{n-1}) \equiv 2 \cdot 1 \pmod n$
Since n is odd, $2 \nmid n$ & $(2, n) = 1$.
So by Cancellation,
$$2^{n-1} \equiv 1 \pmod n.$$

($\Leftarrow$) Suppose
$$2^{n-1} \equiv 1 \pmod n.$$
Then $n \mid 2^{n-1} - 1$. This implies
that n is odd since if $2 \mid n$, $2 \mid 2^{n-1} - 1$,
i.e. $2 \mid 2^{n-1} - (2^{n-1} - 1) = 1$ which is a contradiction
Also
$$2^n = 2 \cdot 2^{n-1} \equiv 2 \cdot 1 \pmod n \text{ &}$$
$$2^n \equiv 2 \pmod n.$$
Hence n is an odd pseudoprime.

(c) Suppose n is an odd pseudoprime.
Then n is odd & composite.
So $a \mid n$ for some $1 < a < n$, $a \in \mathbb{Z}$
Hence
$$2^a - 1 \mid 2^n - 1 = n \quad \text{by (a)}$$

And m is composite since
$2 \leq a < n$ & $3 \leq 2^a - 1 < 2^n - 1 = m$.
We need to show
$$2^{m-1} \equiv 1 \pmod{m}.$$
Since n is pseudoprime & odd
$$2^n \equiv 2 \pmod{n}$$
& $n \mid 2^n - 2 = (2^n - 1) - 1 = m - 1$.
By (a)
$$m = 2^n - 1 \mid 2^{m-1} - 1 \quad \&$$
$$2^{m-1} \equiv 1 \pmod{m}.$$
Hence m is an odd pseudoprime by (b).

(d) Let $a_1 = 341$, $a_{n+1} = 2^{a_n} - 1$ for $n \geq 1$.
$a_1 < a_2 < a_3 < \cdots$
since $2^m - 1 > m$ for $m > 2$
(use induction). Since $a_1 = 341$ is
an odd pseudoprime this gives an infinite
sequence of odd pseudoprimes by (c).
Hence there are infinitely many odd pseudoprimes.

Sec'n 26

(p.10)

#68(c) (p.72)

$$\phi(14) = \phi(2)\phi(7) = 1 \cdot 6 = 6.$$

Since $(3, 14)$, we have

$$3^6 \equiv 1 \pmod{14},$$

by Euler's Theorem. We divide 6 into 1000000:

$$1000000 = (166666)(6) + 4.$$

Therefore,

$$\begin{aligned} 3^{1000000} &\equiv (3^6)^{166666} 3^4 \pmod{14} \\ &\equiv 1 \cdot 3^4 \pmod{14} \\ &\equiv 81 \pmod{14} \\ &\equiv 11 \pmod{14}, \end{aligned}$$

since $81 - 11 = 14 \cdot 5$.

71

(a) Suppose $n \in \mathbb{Z}$ & $3 \nmid n$.

& $(n, 9) = 1$ &

$$n^6 \equiv 1 \pmod 9$$

by Euler's Thm since $\varphi(9) = 9 - 3 = 6$.

& $n n^6 \equiv n \pmod 9$, &

$$n^7 \equiv n \pmod 9.$$

By Corollary & FL.7 $n^7 \equiv n \pmod 7$.

So

$$m \mid n^7 - n \quad \text{for} \quad m = 7, 9.$$

Since $(7, 9) = 1$, $63 = 7 \cdot 9 \mid n^7 - n$ &

$$n^7 \equiv n \pmod{63}.$$

(b) Let $n \in \mathbb{Z}$, $9 \mid n$.

Then $n \equiv 0 \pmod 9$ & $n^7 \equiv 0^7 \equiv 0 \equiv n \pmod 9$ &

$n^7 \equiv n \pmod 9$.

By Co. & FLT $n^7 \equiv n \pmod 7$,

since 7 is prime. So

$a \mid n^7 - n$ & $7 \mid n^7 - n$ &

$63 = 9 \cdot 7 \mid n^7 - n$ since $(7, 9) = 1$.

$\therefore$ $n^7 \equiv n \pmod{63}$.

#73 Let m, n be positive relatively prime integers.

Since $(m, n) = 1$

$n^{\varphi(m)} \equiv 1 \pmod m$

by Euler's Thm.

Since $\varphi(m) \geq 1$, $m^{\varphi(m)} \equiv 0 \pmod m$ &

$m^{\varphi(m)} + n^{\varphi(m)} \equiv 0 + 1 \equiv 1 \pmod m$.

By Symmetry, $n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod n$.

So $m \mid m^{\varphi(n)} + n^{\varphi(m)} - 1$ & $n \mid m^{\varphi(n)} + n^{\varphi(m)} - 1$,

&

$mn \mid m^{\varphi(n)} + n^{\varphi(m)} - 1$ since $(m, n) = 1$.

$\therefore$ $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}$.

, #75 (p.72)

LEMMA: Let m be a positive integer with $m > 2$. If a is a positive integer less than m with $(a, m) = 1$, then $(m - a, m) = 1$.

Proof of Lemma: Suppose d is a positive integer and $d \mid (m - a)$ and $d \mid m$.

Then $d \mid (m - (m - a))$ and $d \mid a$. Hence $d = 1$ since $(a, m) = 1$. □

Proof of # 75:

The result is clearly true for $m = 1$. So let m be a positive integer greater then 2. Let $\{r_1, r_2, ...r_k\}$ be a reduced residue system mod m, where $k = \phi(m)$.

We can assume each r_j satisfies $1 \leq r_j < m$.

For each r_i, $(r_i, m) = 1$ and $(m - r_i, m) = 1$ by the Lemma, and we also note that $1 \leq m - r_i < m$. Hence $m - r_i = r_j$ for some unique j. If $i = j$ then $m = 2r_i$ which is impossible since $m > 2$ ($m = 2r_i$ implies $r_i \mid m$, so $r_i = 1$ since $(r_i, m) = 1$; and $m = 2$). Thus for each i there is a unique j not equal to i such that $m - r_i = r_j$ and $r_i + r_j = m \equiv 0 \pmod{m}$.

Hence the numbers $r_1, r_2, \ldots, r_k$ can be partitioned into pairs r_i, r_j such $r_i + r_j \equiv 0 \pmod{m}$.

Therefore,

$$r_1 + r_2 + \cdots r_k \equiv 0 \pmod{m}.$$

□