Homework 2, Math 4150

1. Exercise Set 1.5, #61. Find the greatest common divisor and the least common multiple of each pair of integers below.

   (a) $2^2 \cdot 3^3 \cdot 5 \cdot 7, \quad 2^2 \cdot 3^2 \cdot 5 \cdot 7^2$
   We have,
   $a = 2^2 \cdot 3^3 \cdot 5 \cdot 7$
   $b = 2^2 \cdot 3^2 \cdot 5 \cdot 7^2$
   So LCM is $2^2 \cdot 3^3 \cdot 5 \cdot 7^2 = 4 \cdot 27 \cdot 5 \cdot 49 = 26460$
   And GCD is $2^2 \cdot 3^2 \cdot 5 \cdot 7 = 1260$

   (b) $2^2 \cdot 5^2 \cdot 7^3 \cdot 11^2, \quad 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17$
   We have,
   $a = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7^3 \cdot 11^2 \cdot 13^0 \cdot 17^0$
   $b = 2^0 \cdot 3 \cdot 5 \cdot 7^0 \cdot 11 \cdot 13 \cdot 17$
   So LCM is $2^2 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 = 2751648900$
   And GCD is $5 \cdot 11 = 55$

   (c) $2^2 \cdot 5^7 \cdot 11^{13}, \quad 3^2 \cdot 7^5 \cdot 13^{11}$
   We have,
   $a = 2^2 \cdot 5^7 \cdot 11^{13}$
   $b = 3^2 \cdot 7^5 \cdot 13^{11}$
   So LCM is $2^2 \cdot 3^2 \cdot 5^7 \cdot 7^5 \cdot 11^{13} \cdot 13^{11} = 2.9245868e + 36$
   And GCD is 1

   (d) $3 \cdot 17 \cdot 19^2 \cdot 23, \quad 5 \cdot 7^2 \cdot 11 \cdot 19 \cdot 29$
   We have,
   $a = 3 \cdot 17 \cdot 19^2 \cdot 23$
   $b = 5 \cdot 7^2 \cdot 11 \cdot 19 \cdot 29$
   So LCM is $3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 17 \cdot 19^2 \cdot 23 \cdot 29 = 33094969215$
   And GCD is 19

2. Exercise Set 1.5, #70. Prove or disprove the following statements.

   (a) If $a, b \in \mathbb{Z}$, $a, b > 0$, and $a^2 \mid b^3$, then $a \mid b$.

   Consider if $a = 8$ and $b = 12$. We have $8 \nmid 12$ however $a^2 = 64$ and $b^3 = 1728$ and we see that $64|1728$ as $64 \cdot 27 = 1728$. This disproves the above statement.

   (b) If $a, b \in \mathbb{Z}$, $a, b > 0$, and $a^2 \mid b^2$, then $a \mid b$.

   Let $a = p_1^{a_1} \dots p_n^{a_n}$ and $b = p_1^{b_1} \dots p_n^{b_n}$ here $a_1, \dots, a_n, b_1, \dots, b_n$ are greater than equal to zero which means that the primes not dividing one of the numbers get exponent zero. Now assume that $a \nmid b$ this means that there is some p_i such that $a_i > b_i$. Now, if we square both the numbers we have the exponent as $2a_i$ and $2b_i$ respectively and we have $2a_i > 2b_i$ which means that $a^2 \nmid b^2$ which is a contradiction. This means our assumption that $a \nmid b$ is wrong which means that $a \mid b$

   (c) If $a \in \mathbb{Z}$, $a > 0$, p is a prime number, and $p^4 \mid a^3$, then $p^2 \mid a$.

   First we write $a = q_1^{a_1} \dots q_n^{a_n} p^k$ where $q_1, \dots, q_n, p$ are prime numbers and $a_1, \dots, a_n > 0$ while $k \geq 0$. This means that p need not be a divisor of a. We know that $p^4|a^3$ which means that,

$$p^4 \mid q_1^{3a_1} \dots q_n^{3a_n} p^{3k}$$

   Now this must mean that $3k \geq 4$ as otherwise p^4 is not in the prime factorization of a which means p^4 does not divide a which we know is not the case. So we have $3k \geq 4$ which means that $k \geq \frac{4}{3}$. However, we know that $a \in \mathbb{Z}$ which must mean that $k \geq 0, k \in \mathbb{Z}$. So if $k \geq \frac{4}{3}$ then we have $k \geq 2$. So we have,

$$a = q_1^{a_1} \dots q_n^{a_n} p^k \quad \text{where } k \geq 2$$

   Now if $k \geq 2$ then it means that p^2 is in the prime factorization of a which means that,

$$p^2 | q_1^{a_1} \dots q_n^{a_n} p^k \implies p^2 | a$$

   which completes our proof.

3. Exercise Set 1.5, #78 Let $n \in \mathbb{Z}$ with $n > 1$. The nth *harmonic number* H_n is defined by $H_n := 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$. Prove that $H_n \notin \mathbb{Z}$.

   Solution.

   Let $l = LCM(1, \ldots, n)$, so we have $H_n = \frac{1}{l}(l + \frac{l}{2} + \cdots + \frac{l}{n})$. We need to show that $l \nmid l + \frac{l}{2} + \cdots + \frac{l}{n}$. Now, we know that for some largest $1 \leq k \leq n$ we have $2^k \mid l$ so we know that l is even. But now consider $l + \frac{l}{2} + \cdots + \frac{l}{n}$. For any $1 \leq m \leq n$ we know that if $m = 2^r d$ where d is odd then if $r < k, m$ has to be even. So the only case where $\frac{l}{m}$ is odd is when in $m = 2^r d$ we have $r = k$. However, the only possible value for this is when $m = 2^r$ where $d = 1$ as else if $d > 1$ then $2^{r+1} \leq n$ which means that r is not the greatest power of 2 such that $2^r \leq n$. So, there is only one integer smaller than n that is divisible by 2^r which means that $\frac{l}{2^r}$ is not divisible by 2, or is odd. As for any other $\frac{l}{m}$ we have $2 \mid \frac{l}{m}$ this means that $l + \frac{l}{2} + \cdots + \frac{l}{n}$ is an odd number as we only have one odd number in that list. But, we know that l is even and we can't have an even number dividing an odd numbers which means that $H_n \notin \mathbb{Z}$.

4. Exercise Set 1.5, #87.

(a) Let $a, b \in \mathbb{Z}$. Prove that if a and b are expressible in the form $6n+1$, where n is an integer, then ab is also expressible in that form.

Solution.

We have $a = 6n+1$ and $b = 6m+1$ which means that $ab = (6n+1)(6m+1) = 36mn + 6n + 6m + 1 = 6(6mn + m + n) + 1 = 6k + 1$ where $k = 6mn + m + n$

(b) Prove that there are infinitely many prime numbers of the form $6n+5$, where n is an integer. (Hint: Parallel the proof of Proposition 1.22 that uses proof by contradiction).

Assume to the contrary that there are not infinitely many primes of the form $6n+5$ so let $p_0 = 5, p_1, \ldots, p_r$ be the finitely many primes of that form. Now consider the number $N = 6p_1 \ldots p_r + 5$. Now N has either primes of the form $6k+1$ or $6k+5$. We know at least one of the primes must be of the form $6k+5$ as otherwise N will be of the form $6k+1$ itself based on (a). Therefore let p_i be the prime of the form $6k+5$. So we have either $5|N$ or $p_i|N$ for some $0 \leq i \leq r$.

Case 1. If $5|N$ then $5|6p_1 \ldots p_n + 5$ so $5|6p_1 \ldots p_n$. But this is not possible as $p_1, \ldots, p_n$ are primes with 5 being not one of them.

Case 2. If $p_i|N$ then we have $p_i|N - 6p_1 \ldots p_n$ as $p_i|6p_1 \ldots p_n$ so $p_i|5$ which is not possible as p_i is a prime greater than 5.

Hence both cases lead to a contradiction. This implies our assumption is wrong and there are infinitely many primes such that $p = 6n+5$.

5. Exercise Set 2.1, #12
Let $a, b, c, d \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Prove or disprove the following statements.

   (a) $(a - c) \equiv (b - d) \pmod{m}$.

   Solution.

   We have $a \equiv b \pmod{m}$ which means $a - b = k_1 m$ and $c \equiv d \pmod{m}$ which means $c - d \equiv k_2 m$. Now subtracting second from the first we have,

$$\begin{aligned} a - c - b + d &= (k_1 - k_2)m \\ a - c - (b - d) &= (k_3)m \end{aligned}$$

   Or that $a - c \equiv b - d \pmod{m}$

   (b) If $c \mid a$ and $d \mid b$, then $\frac{a}{c} \equiv \frac{b}{d} \pmod{m}$.

   Solution.

   Let $a = 33$ and $b = 12$ so we have $33 - 12 = 21$ so $a \equiv b \pmod{3}$ now take $c = 3$ and $d = 3$ so we have $c - d = 0$ so $c \equiv d \pmod{3}$. We also have $c \mid a$ as $3 \mid 33$ as well as $d \mid b$ or $3 \mid 12$. However we see that $\frac{a}{c} = 11$ and $\frac{b}{d} = 4$ but $11 - 4 = 7$ and $3 \nmid 7$ which means that $\frac{a}{c} \not\equiv \frac{b}{d} \pmod{m}$

6. Exercise Set 2.1 #13

(a) Let a be an even integer. Prove that $a^2 \equiv 0 \pmod 4$.

Solution.

If a is an even integer than $a = 2m$ for some $m \in \mathbb{Z}$. So we have $a^2 = (2m)^2 = 4m^2$. So $4 \mid 4m^2$ or $4m^2 - 0 = 4k$ or $4m^2 \equiv 0 \pmod 4$

(b) Let a be an odd integer. Prove that $a^2 \equiv 1 \pmod 8$. Deduce that $a^2 \equiv 1 \pmod 4$.

Solution.

If a then a can be written as $a = 2m + 1$ for some $m \in \mathbb{Z}$. Now $a^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 4m(m + 1) + 1$. If m is odd then $m + 1$ is even, else m is even. In both cases either m or $m + 1$ is even so take it as $2k$ for some $k \in \mathbb{Z}$. So we have $a^2 = 8k(m + 1) + 1$ or $a^2 = 8km + 1$. In both cases we can write $a^2 = 8z + 1$ for some z. This gives us $8z + 1 \equiv 1 \pmod 8$ as $8 \mid 8z$ which means that $a^2 \equiv 1 \pmod 8$.

Now if $a^2 \equiv 1 \pmod 8$ we have $8 \mid a^2 - 1$. But this implies that $4 \mid a^2 - 1$ as 4 is a factor for 8. Hence we get $a^2 \equiv 1 \pmod 4$.

(c) Prove that if n is a positive integer such that $n \equiv 3 \pmod 4$, then n can't be written as the sum of two square integers.

Solution. We can write any arbitrary integer as $a = 2k$ or $a = 2k + 1$. Now if we square both of them we get $a^2 = 4k^2$ and $a^2 = 4k^2 + 1 + 4k = 4k' + 1$. In both cases we have the square is congruent to either 0 or 1 modulo 4. But this means that the sum of two squares can only be congruent to either $0 + 0, 0 + 1, 1 + 1$ modulo 4 which means that we can't find a sum of two squares n to be congruent to 3 modulo 4.

(d) Prove or disprove the converse of the statement in part (c) above.

Solution.

The converse of the statement is that if n can't be written as the sum of two square integers then $n \equiv 3 \pmod 4$. Consider $n = 12$. We cannot write n as the sum of two squares as 12 can only be made using $(1 + 11, 2 + 10, 3 + 9, 4 + 8, 5 + 7, 6 + 6)$ which do not consist a sum of squares. However, at the same time 12 is divisible by 4 which means it does not leave remainder 3 modulo 4.

7. Exercise Set 2.2, #29 (b),(d),(f). Find the inverse modulo m of each integer n below.

   (a) $n = 8$, $m = 35$.

   Solution.

   We need to find the inverse modulo m of 8, or x such that $8x \equiv 1 \pmod{35}$. We have,

   $$\begin{aligned} 35 &= 8 \cdot 4 + 3 \\ 8 &= 3 \cdot 2 + 2 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}$$

   This gives us $2 = 3 - 1$ so $8 = 3 \times 2 + 3 - 1 = 3 \times 3 - 1$ so $35 = 8 \times 4 + \frac{8+1}{3}$ or that,

   $$35 \times 3 + 8 \times (-13) = 1$$

   So we have $x = -13$ such that $8x = 8 \times -13 \equiv 1 \pmod 35$

   (b) $n = 51$, $m = 99$.

   We see that $gcd(51, 99) > 1$. Hence 55 does not have an inverse modulo 99.

   (c) $n = 1333$, $m = 1517$.

   We have,

   $$\begin{aligned} 1517 &= 1333 \times 1 + 184 \\ 1333 &= 184 \times 7 + 45 \\ 184 &= 45 \times 4 + 4 \\ 45 &= 4 \times 11 + 1 \end{aligned}$$

   So we have $4 = \frac{45-1}{11}$ So $184 \times 11 = 45 \times 45 - 1$, $1333 \times 45 = 184 \times (326) + 1$. And, $1 = 1333 \times 371 + 1517 \times -326$.

   So we have $x = 371$ such that $1333x = 1333 \times 371 \equiv 1 \pmod{1517}$.

8. Exercise Set 2.3, #33(a),(e), 34 (b) Find the least non-negative solution of each system of congruences below.

(a)

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 2 \pmod 5 \end{aligned}$$

Solution.
Let $M = 4 \cdot 5 = 20$ so we have $M_1 = 5$ and $M_2 = 4$. Now we solve,

$$\begin{aligned} 5x_1 &\equiv 1 \pmod 4 \\ 4x_2 &\equiv 1 \pmod 5 \end{aligned}$$

We have $5 - 4 = 1$. So inverse of 5 mod 4 is 1 and inverse of 4 mod 5 is -1. So we have $x_1 = 1$ and $x_2 = -1$ by inspection. Now to construct our solution we have,

$$x = b_1 M_1 x_1 + b_2 M_2 x_2 = 3 \cdot 5 \cdot 1 + 2 \cdot 4 \cdot -1 = 15 - 8 = 7$$

(b)

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 6 \pmod 7 \end{aligned}$$

Solution.
Let $M = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ so we have $M_1 = 105, M_2 = 70, M_3 = 42, M_4 = 30$. Now we solve,

$$\begin{aligned} 105x_1 &\equiv 1 \pmod 2 \\ 70x_2 &\equiv 1 \pmod 3 \\ 42x_3 &\equiv 1 \pmod 5 \\ 30x_4 &\equiv 1 \pmod 7 \end{aligned}$$

We have the following,

$$\begin{aligned} 105 - 2 \cdot 52 &= 1 \\ 70 - 3 \cdot 23 &= 1 \\ 5 \cdot 17 - 42 \cdot 2 &= 1 \\ 7 \cdot 13 - 3 \cdot 30 &= 1 \end{aligned}$$

So we have $x_1 = 1, x_2 = 1, x_3 = -2, x_4 = -3$ which gives us,

$$\begin{aligned} x &= b_1M_1x_1 + b_2M_2x_2 + b_3M_3x_3 + b_4M_4x_4 \\ &= 1 \cdot 105 + 2 \cdot 70 + 4 \cdot 42 \cdot -2 + 6 \cdot 30 \cdot -3 \\ &= 105 + 140 - 336 - 540 \\ &= -631 \end{aligned}$$

Now, $-631 \equiv -1 \pmod 2)10$. So the least non-negative number is 209

(c)

$$\begin{aligned} 3x &\equiv 2 \pmod 4 \\ 4x &\equiv 1 \pmod 5 \\ 6x &\equiv 3 \pmod 9 \end{aligned}$$

Solution.
First we can rewrite $6x \equiv 3 \pmod 9$ to $2x \equiv 1 \pmod 3$ and we have, $4 - 3 = 1, 5 - 4 = 1$ and $3 - 2 = 1$. This gives us the following,

$$\begin{aligned} x &\equiv -2 \equiv 2 \pmod 4 \\ x &\equiv -1 \equiv 4 \pmod 5 \\ x &\equiv -1 \equiv 2 \pmod 3 \end{aligned}$$

Now we have $M = 4 \cdot 5 \cdot 3 = 60$ or $M_1 = 15, M_2 = 12, M_3 = 20$. We need to solve,

$$\begin{aligned} 15x_1 &\equiv 1 \pmod 4 \\ 12x_2 &\equiv 1 \pmod 5 \\ 20x_3 &\equiv 1 \pmod 3 \end{aligned}$$

We have $4 \cdot 4 - 15 = 1$, $5 \cdot 5 - 2 \cdot 12 = 1$ and $7 \cdot 3 - 20 = 1$. Which gives us,

$$x_1 = -1, x_2 = -2, x_3 = -1$$

so,

$$\begin{aligned} x &= b_1M_1x_1 + b_2M_2x_2 + b_3M_3x_3 \\ &= 2 \cdot 15 \cdot -1 + 4 \cdot 12 \cdot -2 + 2 \cdot 20 \cdot -1 = -30 - 96 - 40 = -166 \end{aligned}$$

180 - Now as $-166 \equiv 14 \pmod{60}$ our smallest positive integer is 14

9. Exercise Set 2.3 #35. There are n eggs in a basket. If eggs are removed from the basket $2, 3, 4, 5$ and 6 at a time, there remain $1, 2, 3, 4$ and 5 eggs in the basket, respectively. If eggs are removed from the basket 7 at a time, no eggs remain in the basket. What is the smallest value of n for which this scenario could occur (Show all of your work)?

   Solution. We have the following equivalencies,

$$\begin{aligned} n &\equiv 1 \pmod 2 \\ n &\equiv 2 \pmod 3 \\ n &\equiv 3 \pmod 4 \\ n &\equiv 4 \pmod 5 \\ n &\equiv 5 \pmod 6 \\ n &\equiv 0 \pmod 7 \end{aligned}$$

First we see that $n \equiv 3 \pmod 4$ means that $n - 3 = 4k$ for some $k \in \mathbb{Z}$ which means that $n - 1 = 4k + 2 = 2(2k + 1) = 2k'$ or that $n \equiv 1 \pmod 2$. Hence, $n \equiv 3 \pmod 4$ implies the other condition so we can ignore the second. Using similar reasoning $n \equiv 5 \pmod 6$ implies $n \equiv 2 \pmod 3$ and hence we don't need to latter condition. So our system of congruence becomes as follows,

$$\begin{aligned} n &\equiv 3 \pmod 4 \\ n &\equiv 4 \pmod 5 \\ n &\equiv 5 \pmod 6 \\ n &\equiv 0 \pmod 7 \end{aligned}$$

Now we see that 4 and 6 are not coprime. Both of them give us, $n - 3 = 4k_1$ and $n - 5 = 6k_2$. Putting value of n from first to the second gives us,

$$\begin{aligned} 4k_1 + 3 - 5 &= 6k_2 \\ 4k_1 - 2 &= 6k_2 \\ 2k_1 - 1 &= 3k_2 \\ 2k_1 &\equiv 1 \pmod 3 \\ k_1 &\equiv 2 \pmod 3 \text{ as 2 is the inverse of 2 mod } 3 k_1 = 3x + 2 \end{aligned}$$

Now putting this back to the first gives us,

$$\begin{aligned} n &= 4k_1 + 3 \\ n &= 4(3x + 2) + 3 \\ n &= 12x + 11 n \equiv 11 \pmod{12} \end{aligned}$$

So our new system of congruence are,

$$\begin{aligned} n &\equiv 4 \pmod{5} \\ n &\equiv 0 \pmod{7} \\ n &\equiv 11 \pmod{12} \end{aligned}$$

So we have $M = 5 \cdot 7 \cdot 12 = 420$ and $M_1 = 84, M_2 = 60, M_3 = 35$ and we solve the following,

$$\begin{aligned} 84x_1 &\equiv 1 \pmod{5} \\ 60x_2 &\equiv 1 \pmod{7} \\ 35x_3 &\equiv 1 \pmod{12} \end{aligned}$$

We have $5 \cdot 17 - 84 = 1, 60 \cdot 2 - 7 \cdot 17 = 1$ and $12 \cdot 3 - 35 = 1$ which gives us $x_1 = -1, x_2 = 2, x_3 = -1$. So our solution is,

$$\begin{aligned} x &= b_1M_1x_1 + b_2M_2x_2 + b_3M_3x_3 \\ &= 4 \cdot 84 \cdot -1 + 0 + 11 \cdot 35 \cdot -1 \\ &= -336 + -385 = -721 \end{aligned}$$

And we have $-721 \equiv 119 \pmod{420}$

10. Exercise Set 2.3, #40. Prove that the system of linear congruences in one variable given by

$$
\begin{aligned}
x &\equiv b_1 \pmod{m_1} \\
x &\equiv b_2 \pmod{m_2} \\
&\vdots \\
x &\equiv b_n \pmod{m_n}
\end{aligned}
$$

is solvable if and only if $(m_i, m_j) \mid b_i - b_j$ for all pairs i, j with $i \neq j$. In this case, prove that each solution is unique modulo $[m_1, m_2, \ldots, m_n]$.

Solution.

($\Rightarrow$) First we show that if it's solvable then we have $(m_i, m_j) \mid b_i - b_j$ for all pairs i, j with $i \neq j$. For i, j we know that,

$$
\begin{aligned}
x &\equiv b_i \pmod{m_i} \\
x &\equiv b_j \pmod{m_j}
\end{aligned}
$$

which can be written as $m_i \mid x - b_i$ and $m_j \mid x - b_j$. Now if $m_i \mid x - b_i$ that means that any of it's divisors also divide $x - b_i$ and as $d = (m_i, m_j)$ is a divisor of both m_i, m_j we have $d \mid x - b_1$ and $d \mid x - b_j$. But if d divides both then d also divides the difference of them which means that, $d \mid (x - b_i) - (x - b_j)$ or that $d \mid b_i - b_j$ which is our desired result.

($\Leftarrow$) Now we know that $(m_i, m_j) \mid b_i - b_j$ for any $i \neq j$ and we need to show there exists a solution x satisfying the above system of linear congruence. Consider i, j and we have the following $d = (m_i, m_j) \mid b_i - b_j$ so $\exists k$ such that $dk = b_i - b_j$. We also know that $d = am_i + bm_j$ for some $a, b \in \mathbb{Z}$ which means that $dk = kam_i + kbm_j$.

Now take $x = b_i - kam_i$. So we have $x - b_i = -kam_i = (-ka)m_i$ which means that $m_i \mid x - b_i$. Similarly we have $x - b_j = b_i - b_j - kam_i = dk - kam_i = kam_i + kbm_j - kam_i = kbm_j$ which means $m_j \mid x - b_j$. So we found a solution x satisfying the two congruency between i, j. Now as we can find a solution for any i, j this means that the linear system is solvable.

To show uniqueness consider we have two solutions x, y that satisfying the linear congruence. So we have $x \equiv b_i \pmod{m}_i$ and $y \equiv b_i \pmod{m}_i$. But this means that $x - y \equiv 0 \pmod{m}_i$ or that $x \equiv y \pmod{m}_i$ which means that x and y are equivalent modulo m_i for any i or in other words is unique modulo m_i.

11. Excercise Set 2.4, #43.

(a) Prove that if p is an odd prime number, then $2(p-3)! \equiv -1 \pmod{p}$.

Solution.

We know from Wilson's theorem that,

$$(p-1)! \equiv -1 \pmod{p}$$

And we know that $(p-1) \equiv -1 \pmod{p}$ and $(p-2) \equiv -2 \pmod{p}$ which gives us,

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

So we have,

$$\begin{aligned}(-1)(-2)(p-3)! &\equiv -1 \pmod{p}\\ 2(p-3)! &\equiv -1 \pmod{p}\end{aligned}$$

Which gives us the desired result.

(b) Find the least non-negative residue of $2(100!) \pmod{103}$.

Solution.

We know that $2(p-3)! \equiv -1 \pmod{p}$ which means that $2(103-3) \equiv -1 \pmod{103}$ and $2(100)! \equiv -1 \pmod{103}$.

So -1 is a residue of $2(100!)$ mod 103. But we want a non-negative residue which in this case would be 102 as we have $-1 \equiv 102 \pmod{103}$. So our residue is 102.

12. Excercise Set 2.4, #48. Let p be an odd prime number. Prove that

$$1^2 3^2 5^2 \cdots (p-4)^2 (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Solution.

We know from Wilson's theorem that,

$$(p-1)! \equiv -1 \pmod{p}$$

And we can write $(p-1)! = 1 \cdot 2 \cdot 3 \ldots (p-3) \cdot (p-2) \cdot (p-1)$. Now note that we have the following,

$$\begin{aligned} 2 &\equiv -(p-2) \pmod{p} \\ 4 &\equiv -(p-4) \pmod{p} \\ &\vdots \\ (p-3) &\equiv -3 \pmod{p} \\ (p-1) &\equiv -1 \pmod{p} \end{aligned}$$

In addition we have $2+(n-1)2 = p-1$ and $n = (p-1)/2$ or in other words $|\{2, \ldots, p-1\}| = (p-1)/2$. So we can write the following,

$$\begin{aligned} (p-1)! &\equiv -1 \pmod{p} \\ (p-1)! &\equiv 1 \cdot 2 \cdot 3 \ldots (p-2) \cdot (p-1) \equiv -1 \pmod{p} \\ 1 \cdot -(p-2) \cdot 3 \ldots (p-2) \cdot -1 &\equiv -1 \pmod{p} \\ 1^2 \cdot 3^2 \cdot 5^2 \ldots (p-4)^2 (p-2)^2 (-1)^{(p-1)/2} &\equiv -1 \pmod{p} \end{aligned}$$

However we also know that the inverse of $-1 \bmod p$ is itself i.e. $-1 \cdot -1 \equiv 1 \pmod{p}$. So the inverse of $-1^{(p-1)/2}$ is itself. So we get,

$$\begin{aligned} 1^2 3^2 5^2 \ldots (p-4)^2 (p-2)^2 &\equiv -1 - 1^{(p-1)/2} \pmod{p} \\ 1^2 3^2 5^2 \ldots (p-4)^2 (p-2)^2 &\equiv -1^{(p+1)/2} \pmod{p} \end{aligned}$$

Which is what we want.