These solutions are written at the request of students. Please let me know if you don't understand these solutions; I'm happy to expand on them if necessary.

2. Let n be an odd number, not necessarily prime. Show that $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$ as follows.

   (a) Write $n = p_1 p_2 \cdots p_k$ as a product of odd (not necessarily distinct) primes. Show that
$$\left(\frac{-1}{n}\right) = (-1)^{\sum_j \frac{p_j-1}{2}}.$$

Solution: We use two facts: first, that
$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_k}\right)$$
and second, that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. (For this second fact, you might be saying to yourself: "Wait a minute, Peter's trying to pull the wool over my eyes. I know that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$, but he's written '=' up there." It's true. But $(-1)^{(p-1)/2} = \pm 1$, and modulo p that's still just ± 1. It really is just an equals, not equal modulo p.)

We use these facts and compute:
$$\begin{aligned}\left(\frac{-1}{n}\right) &= \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_k}\right)\\ &= (-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_2-1}{2}}\cdots(-1)^{\frac{p_k-1}{2}}\\ &= (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_k-1}{2}}\\ &= (-1)^{\sum_j \frac{p_j-1}{2}},\end{aligned}$$
which is what we wished to prove.

   (b) Write $n = p_1 p_2 \cdots p_k$ as
$$n = (1 + (p_1 - 1))(1 + (p_2 - 1))\cdots(1 + (p_k - 1))$$
and show that this simplifies to
$$n = 1 + \sum_{j=1}^{k}(p_j - 1) + 4K \qquad (*)$$
for some integer K. (Use the fact that each p_j is odd, so $p_j - 1$ is even. You may assume that there are at least two primes – so $k \geq 2$ – as the $k = 1$ case is simply $n = p_1$.)

Solution: Let's use induction on k, the number of prime factors of n. Our base case will be $k = 2$, and we can do this by hand:

$$n = (1 + (p_1 - 1))(1 + (p_2 - 1)) = 1 + [(p_1 - 1) + (p_2 - 1)] + (p_1 - 1)(p_2 - 1).$$

Since p_1 and p_2 are both odd primes, we can write $p_1 - 1 = 2k_1$ and $p_2 - 1 = 2k_2$ for integers k_1 and k_2. Thus the above equation for n turns into

$$n = 1 + \sum_{j=1}^{2}(p_j - 1) + 4(k_1k_2),$$

which is equation $(*)$ with $K = k_1k_2$.

Now we assume that equation $(*)$ holds for k and prove it holds for $k+1$ as well. Suppose $n = p_1p_2 \cdots p_kp_{k+1}$ is the product of $k+1$ odd primes. Then, by the induction hypothesis, we can write

$$p_1p_2 \cdots p_k = 1 + \sum_{j=1}^{k}(p_j - 1) + 4K$$

for some integer K. Now, to get n, we multiply both sides by p_{k+1}. That is, we multiply the left-hand side by p_{k+1} and the right-hand side by $1 + (p_{k+1} - 1)$:

$$\begin{aligned} n = p_1p_2 \cdots p_kp_{k+1} &= \left(1 + \sum_{j=1}^{k}(p_j - 1) + 4K\right)(1 + (p_{k+1} - 1)) \\ &= 1 + \sum_{j=1}^{k}(p_j - 1) + 4K \\ &\quad + (p_{k+1} - 1) + (p_{k+1} - 1)\sum_{j=1}^{k}(p_j - 1) + 4K(p_{k+1} - 1) \\ &= 1 + \sum_{j=1}^{k+1}(p_j - 1) + 4K', \end{aligned}$$

where

$$4K' = 4K + (p_{k+1} - 1)\sum_{j=1}^{k}(p_j - 1) + 4K(p_{k+1} - 1).$$

(Clearly the first and last terms on the right-hand side are multiples of 4. The middle term on the right is, as before, a product of two even numbers, and so also a multiple of 4.) This finishes the proof.

(c) Conclude from part (b) that $(-1)^{\sum_j \frac{p_j - 1}{2}} = (-1)^{(n-1)/2}$, so that $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

Solution: Part (b) tells us that

$$n = 1 + \sum_{j=1}^{k}(p_j - 1) + 4K$$

or, equivalently,

$$\frac{n-1}{2} = \frac{1}{2}\sum_{j=1}^{k}(p_j - 1) + 2K = \sum_{j=1}^{k}\frac{p_j - 1}{2} + 2K.$$

This is our exponent for -1; we get

$$\begin{aligned}(-1)^{\frac{n-1}{2}} &= (-1)^{\sum_{j=1}^{k}\frac{p_j-1}{2}+2K}\\ &= (-1)^{\sum_{j=1}^{k}\frac{p_j-1}{2}}(-1)^{2K}\end{aligned}$$

The second term on the right-hand side is -1 raised to an even power, which is 1. Thus we've proved that $(-1)^{(n-1)/2} = (-1)^{\sum_{j=1}^{k}(p_j-1)/2}$, which is the first identity we wish to prove. By part (a), we know that this last expression is $\left(\frac{-1}{n}\right)$, so $(-1)^{(n-1)/2} = \left(\frac{-1}{n}\right)$, as desired.