DMA Practice problems: Calculations modulo

Exercise 1: For the given n and a, find the opposite number $(-a)$ and the inverse number a^{-1} in the space $\mathbb{Z}_n$.

(i) $n = 35$, $a = 12$;

(ii) $n = 36$, $a = 15$;

(iii) $n = 42$, $a = 25$;

(iv) $n = 146$, $a = 75$.

Exercise 2: Evaluate the following expressions in the given $\mathbb{Z}_n$. First rewrite subtraction as addition with opposite elements.

(i) $(7 + 8)^{146} - 1$ modulo $n = 13$;

(ii) $(11 \cdot 27 - 14)^{116}$ modulo $n = 23$;

(iii) $(31 \cdot 4 - 1)^{192}$ modulo $n = 20$;

(iv) $(30 + 31)^{108} - 2$ modulo $n = 53$.

Solution 1:

(i): $(-a) = n - a = 35 - 12 = 23$,
we want $x \in \mathbb{Z}$ so that $12x + 35k = 1$ for some $k \in \mathbb{Z}$,
we use the Euclidean algorithm for that.
We found $3 \cdot 12 + (-1) \cdot 35 = 1$,
modulo 35 this yields $3 \cdot 12 \equiv 1$.
So $12^{-1} = 3$.

35		1	0
12	2	0	1
11	1	1	-2
1•	11	-1•	3•
0			

(ii): $(-a) = 36 - 15 = 21$,
we want $x \in \mathbb{Z}$ so that $15x + 36k = 1$ for some $k \in \mathbb{Z}$,
we use the Euclidean algorithm for that.
We found $\gcd(15, 36) > 1$,
hence 15^{-1} does not exist in $\mathbb{Z}_{36}$.

36		1	0
15	2	0	1
6	2	1	-2
3•	2	-2•	5•
0			

(iii): $(-a) = 42 - 25 = 17$,
we want $x \in \mathbb{Z}$ so that $25x + 42k = 1$ for some $k \in \mathbb{Z}$,
we use the Euclidean algorithm for that.
We found $(-5) \cdot 25 + 3 \cdot 42 = 1$,
modulo 42 this yields $(-5) \cdot 25 \equiv 1$.
We shift $-5 + 42 = 37$, so $25^{-1} = 37$.

42		1	0
25	1	0	1
17	1	1	-1
8	2	-1	2
1•	8	3•	-5•
0			

(iv): $(-a) = 146 - 75 = 71$,
we want $x \in \mathbb{Z}$ so that $75x + 146k = 1$ for some $k \in \mathbb{Z}$,
we use the Euclidean algorithm for that.
We found $(-19) \cdot 146 + 37 \cdot 75 = 1$,
modulo 146 this yields $37 \cdot 75 \equiv 1$.
So $75^{-1} = 37$.

146		1	0
75	1	0	1
71	1	1	-1
4	17	-1	2
3	1	18	-35
1•	3	-19•	37•
0			

Solution 2: Since human computers find it easier to calculate $8 \cdot 9 = 72 \equiv 2$ rather than directly $8 \cdot 9 = 2$ in $\mathbb{Z}_{10}$, we will in this solution do calculations in $\mathbb{Z}$ with congruences.
(i): $\equiv (7+8)^{146} + 12 = 15^{146} + 12 \equiv 2^{146} + 12 = 2^{12\cdot 12+2} + 12 = (2^{12})^{12} \cdot 2^2 + 12$
$\overset{\text{mF}}{\equiv} 1^{12} \cdot 4 + 12 = 16 \equiv 3 \pmod{13}$.
The calculation is valid as $\gcd(2, 13) = 1$ and 13 is a prime.
If we did our calculations in $\mathbb{Z}_{13}$, we would have writen
$\equiv (7+8)^{146} + 12 = 2^{146} + 12 = 2^{12\cdot 12+2} + 12 = (2^{12})^{12} \cdot 2^2 + 12 \overset{\text{mF}}{\equiv} 1^{12} \cdot 4 + 12 = 3$.
(ii): $\equiv (11 \cdot 4 + 9)^{116} = 53^{116} \equiv 7^{116} = 7^{22\cdot 5+14} = (7^{22})^5 \cdot 7^{14} \overset{\text{mF}}{\equiv} 1^5 \cdot 7^{14} = 7^{14} = (7^2)^7$
$= 49^7 \equiv 3^7 = 3^6 \cdot 3 = (3^3)^2 \cdot 3 = 27^2 \cdot 3 \equiv 4^2 \cdot 3 = 16 \cdot 3 = 48 \equiv 2 \pmod{23}$.
The calculation is valid as $\gcd(7, 23) = 1$ and 23 is a prime.
(iii): $= (31 \cdot 4 + 19)^{192} \equiv (11 \cdot 4 + 19)^{192} = (44 + 19)^{192} \equiv (4 + 19)^{192} = 23^{192} \equiv 3^{192}$.
We cannot apply the little fermat (20 is not a prime). Two options.
Reduction of power:
$3^{192} = 3^{3\cdot 64} = (3^3)^{64} = 27^{64} \equiv 7^64 = (7^2)^32 \equiv 9^{32} = (9^2)^{16} \equiv 1^{16} = 1 \pmod{20}$.
Euler: $\varphi(20) = \varphi(2^2 \cdot 5) = 20\big(1 - \frac{1}{2}\big)\big(1 - \frac{1}{5}\big) = 8$, also $\gcd(3, 20) = 1$, hence
$3^{192} = 3^{8\cdot 24} = (3^8)^{24} \equiv 1^{24} = 1 \pmod{20}$.
(iv): $\equiv (30 + 31)^{108} + 51 = 61^{146} + 51 \equiv 8^{108} + 51 = 2^{52\cdot 2+4} + 51 = (8^{52})^2 \cdot 8^4 + 51$
$\overset{\text{mF}}{\equiv} 1^2 \cdot (8^2)^2 + 51 = 64^2 + 51 \equiv 11^2 + 51 = 121 + 51 \equiv 13 \pmod{53}$.
The calculation is valid as $\gcd(8, 53) = 1$ and 53 is a prime.