1. Write down formulas for an isomorphism and its inverse in case $\mathbb{Z}_6 \times \mathbb{Z}_{20} \simeq \mathbb{Z}_{10} \times \mathbb{Z}_{12}$.

Novosad Ivan

$$\begin{tikzcd}
\mathbb{Z}_6 \times \mathbb{Z}_{20} \arrow[rr, "\varphi"] \arrow[d, "\cong\ \varphi_1"'] & & \mathbb{Z}_{10} \times \mathbb{Z}_{12} \\
\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \arrow[rr, "\simeq"', "\varphi_2"] & & \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \arrow[u, "\cong\ \varphi_3"']
\end{tikzcd}$$

$\mathbb{Z}_2 \times \mathbb{Z}_5 \to \mathbb{Z}_{10}$: $u \cdot 2 + v \cdot 5 = 1 \to u = 3,\ v = -1$

$(a, b) \to (a \cdot (-1) \cdot 5 + b \cdot 3 \cdot 2) = (-5a + 6b)$ mod 10

$\mathbb{Z}_3 \times \mathbb{Z}_4 \to \mathbb{Z}_{12}$: $u \cdot 3 + v \cdot 4 = 1 \quad u = 3,\ v = -2$

$(a, b) \to (a \cdot 4 \cdot (-2) + b(3)(3)) = (-8a + 9b)$ mod 12

$$\underset{6\ \ 20}{\varphi(a,b)} \overset{\varphi_1}{\mapsto} \underset{2\ \ 3\ \ 4\ \ 5}{(a, a, b, b)} \overset{\varphi_2}{\mapsto} (a, b, b, a) \overset{\varphi_3}{\mapsto} (\underset{10}{-5a + 6b}, \underset{12}{-8b + 9a})$$

φ

$$\begin{tikzcd}
\mathbb{Z}_6 \times \mathbb{Z}_{20} & & \mathbb{Z}_{10} \times \mathbb{Z}_{12} \arrow[ll, "\psi"'] \arrow[d, "\cong\ \psi_1"] \\
\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \arrow[u, "\cong\ \psi_3"] & & \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \arrow[ll, "\simeq", "\varphi_2"']
\end{tikzcd}$$

$\mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathbb{Z}_6$: $u \cdot 2 + v \cdot 3 = 1 \to u = 2,\ v = -1$

$(a, b) \to (-3a + 4b)$
6

$\mathbb{Z}_4 \times \mathbb{Z}_5 \to \mathbb{Z}_{20}$: $u \cdot 4 + v \cdot 5 = 1 \to u = 4,\ v = -3$

$(a, b) \to (-15a + 16b)$

$$\psi(a,b) \overset{\psi_1}{\mapsto} (a, a, b, b) \overset{\psi_2}{\mapsto} (a, b, b, a) \overset{\psi_3}{\mapsto} (\underset{6}{-3a + 4b}, \underset{20}{-15b + 16a})$$

ψ

2. Find all generators of the group $\mathbb{Z}_{49}^*$.

Since 49 is a prime power p^2, where $p=7$, and the group of units $U(\mathbb{Z}_{49}^*)$ (i.e. the set of all invertible element under multiplication mod 49) is of order $p^2-p=49-7=42$.

Therefore, we are looking for elements with order 42 in $\mathbb{Z}_{49}^*$.

The order of an element a in finite group is the smallest positive integer s.t. $a^m \equiv 1 \pmod{49}$. An element a is a generator of $\mathbb{Z}_{49}^*$ if it's order equal to the order of the group, which is 42 in this case.

Hence generators of $\mathbb{Z}_{49}^*$ are: 3, 5, 10, 12, 17, 24, 26, 33, 38, 40, 45, 47

and since $\varphi(42)=12$, that's all. (φ is euler function)

Thus $\mathbb{Z}_{49}^* = \langle 3 \rangle = \langle 5 \rangle = \langle 10 \rangle = \langle 12 \rangle = \langle 17 \rangle = \langle 24 \rangle = \langle 26 \rangle = \langle 33 \rangle = \langle 38 \rangle = \langle 40 \rangle = \langle 45 \rangle = \langle 47 \rangle$

3. Let G be $\mathbb{Z}_{29}^*$ with $g = 2$ being its generator. The size of the group G is enough to encode the English alphabet, space and period. We will use the following table

a	b	c	d	e	f	g	h	i	j	k	l	m	n
1	2	3	4	5	6	7	8	9	10	11	12	13	14

o	p	q	r	s	t	u	v	w	x	y	z		.
15	16	17	18	19	20	21	22	23	24	25	26	27	28

Your lover sent you the public key $s = g^b = 12$. You chose a to be 10.

(a) Compute the private key $k = g^{ab}$.

(b) Decrypt the message from your lover $20, 2, 6, 28, 15, 9, 2, 4, 14, 8$.

a) $g^{ab} = 12^{10}\ (29)$; $g^{ab} = 28 = k$

b) To compute k^{-1}, let's use $a^{|\mathbb{Z}_{29}^*|} = 1 \rightarrow a \cdot \underbrace{a^{|\mathbb{Z}_{29}^*|-1}}_{a^{-1} = a^{27}} = 1$

$k^{-1} = 28^{-1} = 28^{27} \equiv 28\ (\text{mod } 29)$

$20 \cdot 28 \equiv 9\ (29)$ $\qquad$ $9 \cdot 28 \equiv 20\ (29)$

$2 \cdot 28 \equiv 27\ (29)$ $\qquad$ $2 \cdot 28 \equiv 27\ (29)$

$6 \cdot 28 \equiv 23\ (29)$ $\qquad$ $4 \cdot 28 \equiv 25\ (29)$

$28 \cdot 28 \equiv 1\ (29)$ $\qquad$ $14 \cdot 28 \equiv 15\ (29)$

$15 \cdot 28 \equiv 14\ (29)$ $\qquad$ $8 \cdot 28 \equiv 21\ (29)$

So I want you! is the message

4. Let G be $\mathbb{Z}_{49}^*$ with $g = 3$ being its generator. The size of the group G is enough to encode the English alphabet. We will use the following table

a	b	c	d	e	f	g	h	i	j	k	l	m
2	4	6	9	11	13	16	18	20	23	25	27	30

n	o	p	q	r	s	t	u	v	w	x	y	z
32	34	37	39	41	44	46	48	3	17	31	45	24

Your lover chose the secret number b to be 7 and you chose your secret number a to be 5.

(a) Compute your public key $r = g^a$.
(b) Compute the public key $s = g^b$ of your lover.
(c) Compute the private key $k = g^{ab}$ and its inverse.
(d) Decrypt the message from your lover $31, 37, 3, 13, 44, 22$.

a) $g^a \equiv 47 (49)$

b) $g^b \equiv 31 (49)$

c) $k = 19 (49)$ $\quad k^{-1} = 19^{-1} = 31 \ (49)$

d) $31 \cdot 31 \equiv 30 (49)$ $\quad 13 \cdot 31 \equiv 11 (49)$

$37 \cdot 31 \equiv 20 \ (49)$ $\quad 44 \cdot 31 \equiv 41 (49)$

$3 \cdot 31 \equiv 44 (49)$ $\quad 22 \cdot 31 \equiv 45 \ (49)$

Anwer: Misery.