1. This question is about baby-step-giant-step.

   (a) Use (only) baby-step-giant-step to compute $a \in \mathbb{Z}$ such that $9^a \equiv 17 \pmod{101}$. You may use without proof that 9 has order 50 in the multiplicative group $\mathbb{F}_{101}^*$.

given:

- $g = 9$
- $\ell = 50$
- $p = 101$

Step 1:

i	0	1	2	3	4	5	6	7	8
$b_i = 9^i \pmod{101}$	1	9	81	22	97	65	80	13	16

Step 2:

j	0	1	2	3	4
$c_j = g^a \cdot g^{-\sqrt{\ell} \cdot j} = 17 \cdot 9^{-8j} \pmod{101}$	17	20	77	49	22

This gives $a = i + \sqrt{\ell}\, j$

$= 3 + 4(8)$

$= \boxed{35}.$

Sure enough, $9^{35} \equiv 17 \pmod{101}$

2. (a) Use (only) Pollard-ρ to compute $a \in \mathbb{Z}$ such that $3^a \equiv 8 \pmod{17}$.

Given: $g = 3$, $p = 17$

Note 3 has order 16, so $\ell = 16$.

We now compute:

i	G_i	b_i	c_i
0	3	1	0
1	9	2	0
2	10	3	0
3	12	3	1
4	2	4	1
5	4	8	2
6	15	8	3
7	11	9	3
8	2	18	6

2

Then

$$a \equiv \frac{b_4 - b_8}{c_8 - c_4} \pmod{16}$$

$$\equiv \frac{-14}{5} \pmod{16} = \boxed{10}.$$

Sure enough, $3^{10} \equiv 8 \pmod{17}$.

3. (a) Using index calculus and a factor base of $\{2, 3, 5\}$, find a such that $31^a \equiv 39 \pmod{107}$.

- $p = 107$ • $g = 31$ • $g^a = 39$ • $n = 3$

j	1	2	3	4	5	6	7	8	...	10
$31^j \pmod{107}$	31	105	45	4	17	99	73	16		75
factors of $31^j \pmod{107}$	31	$3\cdot5\cdot7$	$3^2\cdot5$	2^2	17	$3^2\cdot11$	73	2^4		$3\cdot5^2$

This gives:

- $31^3 \equiv 3^2 \cdot 5 \pmod{107}$
  $\implies 3 = 2\log_{31}(3) + \log_{31}(5) \pmod{106}$
- $31^4 = 2^2 \pmod{107}$ ← true
  $\implies 4 \equiv 2\log_{31}(2) \pmod{106}$ true

note
$4 \equiv 2(55) \pmod{106}$
And
$4 \equiv 2(2) \pmod{106}$

- $31^{10} = 3 \cdot 5^2 \pmod{107}$
  $\implies 10 = \log_{31}(3) + 2\log_{31}(5) \pmod{106}$

$31^2 \equiv -2 \pmod{107}$
should be 55

We then solve:

- $\log_{31}(2) \equiv 2 \pmod{106}$
- $\log_{31}(3) \equiv 34 \pmod{106}$
- $\log_{31}(5) \equiv 41 \pmod{106}$

these are right

j	0	1
$31^j \cdot 39$	$3 \cdot 13$	2^5

$$\implies 31 \cdot 39 \equiv 2^5 \pmod{107}$$

$$\implies 1 + \log_{31}(39) \equiv 5 \log_{31}(2) \pmod{106}$$

$$\implies \log_{31}(39) \equiv 5 \log_{31}(2) - 1 \pmod{106}$$

$$\equiv 5(2) - 1$$

$$\equiv 9$$

wrong –

$31^9 \equiv 68 \pmod{107}$

should be 62

(b) How would you alter the algorithm as given in the lecture notes to include a non ad-hoc way of choosing a factor base?

According to Wikipedia: can choose -1, and the first n primes starting at 2 (for any desired value of n)

4. (a) Using SageMath, check that $g = 1178$ is a multiplicative generator of $\mathbb{F}_{2027}^*$.

Mod(1178, 2027).multiplicative_order() == 2026, which confirms that g is a generator.

✓

(b) Using SageMath and baby-step-giant-step, compute a in $\mathbb{Z}$ such that $1178^a = 1728 \pmod{2027}$.

a = 1736 (used the function I wrote for coursework)

✓

(c) Using SageMath and Pollard-rho, re-solve part (b).

used function I made for coursework; got same result