1. $\because x = a, x = b$ are both integer solutions to the congruence $g^x \equiv h(mod\ p)$

   $\therefore g^a \equiv g^b (mod\ p)$

   $\therefore g^{a-b} \equiv 1(mod\ p)$

   g is a generator for Z_p^*, so $g \in Z_p^*$.

   From Fermat's theorem, then

   $g^{p-1} \equiv 1(mod\ p)$

   $\therefore p - 1 | a - b$

   $\therefore a \equiv b(mod\ p - 1)$

2. a) 7. b) 11. c) 18

```python
def simple_program(e, n, p):
    for i in range(0, p):
        if pow(e, i) % p == n:
            return i


print(simple_program(2, 13, 23))
print(simple_program(10, 22, 47))
print(simple_program(627, 608, 941))
```

```
7
11
18
```

3. a) $\tau\sigma^2 = \sigma^2\tau\sigma = \sigma^2\sigma^2\tau = \sigma^3\sigma\tau = \sigma\tau$

   b) $\tau(\sigma\tau) = \tau\sigma\tau = \sigma^2\tau^2 = \sigma^2$

c) $(\sigma\tau)(\sigma\tau) = \sigma\tau\sigma\tau = \sigma\sigma^2\tau\tau = \sigma^3\tau^2 = e$

d) $(\sigma\tau)(\sigma^2\tau) = \sigma\tau\tau\sigma = \sigma\tau^2\sigma = \sigma^2$

Answer: S3 is NOT a commutative group.

Prove:

$If\ S3\ is\ a\ commutative\ group, then\ for\ \forall a, b \in S3, ab = ba. But,$

$$\tau\sigma = \sigma^2\tau = \sigma(\sigma\tau) \neq \sigma\tau$$

$So, S3\ is\ \boldsymbol{NOT}\ a\ commutative\ group.$

4. $\because\ a \in Z_p^*$, from Fermat's theorem, then

$a^{p-1} \equiv 1\ (mod\ p)$

$\because\ b = a^{\frac{p-1}{q}}$

$\therefore\ b^q = a^{p-1} \equiv 1\ (mod\ p)$

$\therefore\ ord_p(b)|q$

But q is a prime,

$\therefore$if $b \neq 1$, then b has order q.

$\therefore$either $b = 1$ or else b has order q.