Problem 1a

$3^2 \equiv 9$
$3^4 = 9^2 \equiv 81 \equiv 4$
$3^8 = 4^2 \equiv 16 \equiv 5$
$3^{16} = 5^2 \equiv 25 \equiv 3$
$3^{32} = 3^2 \equiv 9 \equiv 9$
$3^{64} = 9^2 \equiv 81 \equiv 4$
$3^{128} = 4^2 \equiv 16 \equiv 5$
$3^{256} = 5^2 \equiv 25 \equiv 3$
$3^{512} = 3^2 \equiv 9 \equiv 9$
$3^{1024} = 9^2 \equiv 81 \equiv 4$

$$3^{1500} \equiv (3^{1024}) \cdot (3^{256}) \cdot (3^{128}) \cdot (3^{64}) \cdot (3^{16}) \cdot (3^{8}) \cdot (3^{4})$$
$$\equiv 4 \times 3 \times 5 \times 4 \times 3 \times 5 \times 4 \equiv 14400$$
$$\equiv 1$$

Problem 1b

$5^2 \equiv 25 \equiv 5$
$5^4 = 5^2 \equiv 25 \equiv 5$
$5^8 = 5^2 \equiv 25 \equiv 5$
$5^{16} = 5^2 \equiv 25 \equiv 5$
$5^{32} = 5^2 \equiv 25 \equiv 5$
$5^{64} = 5^2 \equiv 25 \equiv 5$
$5^{128} = 5^2 \equiv 25 \equiv 5$
$5^{256} = 5^2 \equiv 25 \equiv 5$
$5^{512} = 5^2 \equiv 25 \equiv 5$
$5^{1024} = 5^2 \equiv 25 \equiv 5$
$5^{2048} = 5^2 \equiv 25 \equiv 5$
$5^{4096} = 5^2 \equiv 25 \equiv 5$

$$5^{4358} \equiv (5^{4096}) \cdot (5^{256}) \cdot (5^{4}) \cdot (5^{2})$$
$$\equiv 5 \times 5 \times 5 \times 5 \equiv 625$$
$$\equiv 5$$

Problem 1c

$6^1 \equiv 6$

$6^2 = 6^2 \equiv 36 \equiv 1$

$6^4 = 1^2 \equiv 1 \equiv 1$

$6^8 = 1^2 \equiv 1 \equiv 1$

$6^{16} \equiv 1$

$6^{32} \equiv 1$

$6^{64} \equiv 1$

$6^{128} \equiv 1$

$6^{256} \equiv 1$

$6^{512} \equiv 1$

$6^{1024} \equiv 1$

$6^{2048} \equiv 1$

$6^{4096} \equiv 1$

$6^{8192} \equiv 1$

$6^{16384} \equiv 1$

$$6^{22345} \equiv (6^{16384}) \cdot (6^{4096}) \cdot (6^{1024}) \cdot (6^{512}) \cdot (6^{256}) \cdot (6^{64}) \cdot (6^4) \cdot (6^4) \cdot (6^1)$$

$$\equiv 1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 6 \equiv 6$$

$$\equiv 6$$

Problem 2a

$$648 = 124 \times 5 + 28$$
$$124 = 28 \times 4 + 12$$
$$28 = 12 \times 2 + 4$$
$$12 = 4 \times 3 + 0$$

$$\begin{aligned} GCD(648, 124) &= GCD(124, 28) \\ &= GCD(28, 12) \\ &= GCD(12, 4) \\ &= 4 \end{aligned}$$

Problem 2b

$$123456789 = 123456788 \times 1 + 1$$
$$123456788 = 1 \times 123456788 + 0$$

$$GCD(123456789, 123456788)$$
$$= GCD(123456788, 1)$$
$$= 1$$

Problem 2c

$$\begin{aligned} 2200 &= 2^3 \times 275 \\ &= 2^3 \times 5^2 \times 11 \end{aligned}$$

$$GCD = 2^{\min(300, 3)} \times 3^{\min(200, 0)} \times 5^{\min(2, 0)} \times 11^{\min(1, 0)}$$
$$GCD = 2^3 \times 3^0 \times 5^0 \times 11^0$$
$$= 8$$

Problem 3

According to the Diffie-Hellman key Exchange
Protocal. Alice and Bob will get the key
$key = (g^x)^y \pmod{p} = (g^y)^x \pmod{p}$
Since Alice wants to send an extra number
to Bob to make the key become the specific number key_s
make that:
$key_s = key +$ Extra number

So Alice will need to calculater the key
and find out the different between key_s & key
$(key_s - key) =$ Extra number..
Alice will need send this Extra number
to Bob.

E.g.:

- Bob & Alice confirmed p & g. eg: $p=23$, $g=5$
- key = share security key eg: 2
  key_s = share security key that Alice want. eg: 5
- Alice think of random x and sends $g^x \pmod{p}$ to Bob
  eg: $x=6$, $g^x \pmod{p} = 5^6 \% 23 = 8$
- Alice Also send an Extra number to Bob.
  and let Bob know that:
  The actual $key_s = key +$ Extra number
  Extra number $= key_s - key$
  $= 5 - 2$
  $= 3$
- Bob think of random y and send $g^y \pmod{p}$ to Alice
  eg: $y=15$, $g^y \pmod{p} = 5^{15} \% 23 = 19$
- Bob caculate the key
  $(g^x)^y \pmod{p} +$ Extra number
  $= 8^{15} \pmod{23} + 3$
  $= 2 + 3$
  $= 5 = key_s$

Problem 4 (Super simple solution)

```python
def countEvents(A, t):
    count = 0
    for i in range(len(A)):
        for j in range(len(A)):
            if i < j and A[i] > t * A[j]:
                count += 1
    return count
```