1. Notice that gnome \( d \) will flip switch \( n \) if and only if \( d \mid n \). Therefore, the number of times that switch \( n \) is flipped is equal to the number of divisors of \( n \) (including 1 and \( n \)).

Examining small cases reveals that the first several numbers with an odd number of divisors are \( 1, 4, 9, 16, 25, \ldots \), suggesting that the switches left "on" are precisely those labeled with perfect squares.

Indeed, this guess is correct. One way to see this is: every divisor \( d \) of \( n \) has a "partner" \( n/d \), unless \( d=n/d \), i.e. \( d=\sqrt{n} \) (which you could regard as being its own partner). So if \( \sqrt{n} \notin \mathbb{Z} \) then the divisors of \( n \) can be paired off, hence there's an even number of them. But if \( \sqrt{n} \in \mathbb{Z} \) (i.e. \( n \) is a square) then \( \sqrt{n} \) is the "odd divisor out" with no partner, so \( n \) has an odd number of divisors.

So one switch is left on for each square less than 1000. Since \( 31^2=961 \) and \( 32^2=1024 \), there are \( 31 \) such switches.

(Addendum: see the last page for a nice visualization from a student)

2. a) Since \( m=pq \) and \( \gcd(p,q)=1 \), CRT shows that
\[
 s^e \equiv s \mod m \iff \text{ both } \quad \begin{align*}
 s^e &\equiv s \mod p \\
 s^e &\equiv s \mod q.
\end{align*}
\]

Now, \( e^p=1 \mod \phi(m) \) and \( \phi(m)=(p-1)(q-1) \), so \( e^p=1 \mod (p-1) \) as well. This implies, by Fermat's little theorem, that
\[
\text{if } \gcd(s,p)=1, \text{ then } s^e \equiv s \mod p.
\]

However, it is also possible that \( \gcd(s,p)=1 \). Since \( p \) is prime, this can only be true if \( p \mid s \), i.e. \( s \equiv 0 \mod p \). But in this case,
\[
 s^e \equiv 0^e \equiv 0 \equiv s \mod p.
\]
So in either case (whether $p \mid s$ or not), $s^{e^p} \equiv s \mod p$.

Exchanging $p \& q$, the same argument shows that $s^{e^q} \equiv s \mod q$.

Therefore for all $s$, $s^{e^p} \& s^{e^q}$ are congruent $\mod p \& q$, hence they are congruent $\mod pq$, as desired.

b) $45 = 3^2 \cdot 5$, so $\varphi(45) = (3^2 - 3) \cdot (5 - 1) = 24$. So if $e = p = 5$ then indeed $e^p = 25 \equiv 1 \mod \varphi(45)$.

However, consider $s = 3$. Then

\[ s^1 \equiv 3 \mod 45 \]
\[ s^2 \equiv 9 \mod 45 \]
\[ s^3 \equiv 27 \mod 45 \]
\[ s^6 \equiv 27^2 = 729 \equiv 9 \mod 45 \]
\[ s^{11} \equiv 81 = -27 \equiv -9 \mod 45 \]
\[ s^{20} \equiv 4 \times 9^2 = 81 = -9 \mod 45 \]
\[ s^{25} \equiv -9 \cdot 3 = -27 \equiv 18 \mod 45 \]

So $s^{e^p} \equiv 18$, while $s \equiv 3 \pmod{45}$. So $p$ does not always "decrypt" $e$.

The other exceptions are $s = 6, 12, 15, 21, 24, 30, 33, 39, 42$. This is because it is always true that $s^{e^p} \equiv s \mod 5$, but anything that is congruent to 3 or 6 $\mod 9$ becomes 0 $\mod 9$ when raised to any power.

3) a) Alice can compute $t$ as $s^{p \cdot \varphi(m)}$. Then

\[ t^e = (s^e)^e \equiv s \mod m, \text{ as desired.} \]

b) Computing $t$ from $s^{e^p}$ amounts to solving

\[ x^e \equiv s \mod m \text{ for } x. \]
This is equivalent to decrypting a message encrypted with RSA. So unless Mallory knows how to crack RSA, she cannot forge a signature for a chosen message $s$.

(4) a) For each prime, just compute squares of the first half of the numbers $1, 2, \ldots, p-1$ and reduce.

- $p = 2$: QRs: 1 mod 2
  NRs: none.
  
- $p = 3$: QRs: 1 mod 3
  NRs: 2 mod 3.
  
- $p = 5$: QRs: 1, 4 mod 5
  NRs: 2, 3 mod 5
  
- $p = 7$: squares 1, 2, 4, 9 reduce to 1, 2, 4, 1, 4, 2.
  QRs: 1, 2, 4
  NRs: 3, 5, 6
  
- $p = 11$: squares 1, 4, 9, 16, 25 reduce to 1, 4, 9, 5, 3
  QRs: 1, 3, 4, 5, 9
  NRs: 2, 6, 7, 8, 10
  
- $p = 13$: squares 1, 4, 9, 16, 25, 36 reduce to 1, 4, 9, 3, 12, 10
  QRs: 1, 3, 4, 9, 10, 12
  NRs: 2, 5, 6, 7, 8, 11
  
- $p = 17$: squares 1, 4, 9, 16, 25, 36, 49, 64 reduce to 1, 4, 9, 16, 8, 2, 15, 13
  QRs: 1, 2, 4, 8, 9, 13, 15, 16
  NRs: 3, 5, 6, 7, 10, 11, 12, 14
\[ p = 19 \]

squares: \(1, 4, 9, 16, 25, 36, 49, 64, 81\)
reduce to: \(1, 4, 9, 16, 6, 17, 11, 7, 5\)

QRs: \(1, 4, 5, 6, 7, 9, 11, 16, 17\)
NRs: \(2, 3, 8, 10, 12, 13, 14, 15, 18\)

b) \[ A(2) = 1 \quad B(2) = 0 \]
\[ A(3) = 1 \quad B(3) = 2 \]
\[ A(5) = 5 \quad B(5) = 5 \quad \leftarrow \]
\[ A(7) = 7 \quad B(7) = 14 \]
\[ A(1) = 22 \quad B(1) = 33 \]
\[ A(13) = 39 \quad B(13) = 39 \quad \leftarrow \]
\[ A(17) = 68 \quad B(17) = 68 \quad \leftarrow \]
\[ A(19) = 76 \quad B(19) = 95 \]

c) It appears that \(A(p) = B(p)\) when \(p \equiv 1 \text{ mod } 4\). Indeed, this is the case for all \(p\). Here is a proof (not part of the homework since it uses material from Friday's class):

Claim 1: If \(p \equiv 3 \text{ mod } 4\) (or \(p = 2\)) then \(A(p) \neq B(p)\).
Proof: Note \(A(p) + B(p) = 1 + 2 + 3 + \cdots + (p-1) = \frac{p(p-1)}{2}\) (sum of an arithmetic series) and \(p(p-1) \equiv 2 \text{ mod } 4\), so \(A(p) + B(p)\) is odd. Thus it's impossible for \(A(p) \) to equal \(B(p)\).

Claim 2: If \(p \equiv 1 \text{ mod } 4\), then \(A(p) = B(p)\).
Proof: If \(p \equiv 1 \text{ mod } 4\), then \(\left(\frac{-1}{p}\right) = 1\), i.e. \(\equiv \equiv\)
p-1 is a QR mod p. So for all \(a\),

\[ a \equiv a \text{ QR } \implies p - a \equiv a \text{ QR } \implies \]

So the QRs are paired off into pairs summing to \(p\).
This means the sum of all of them is \(\# \text{QRs} \cdot \frac{p+1}{2}\).
The same is true of the NRs. So both sum \(A(p)\) & \(B(p)\) are equal to \(\frac{p+1}{2}\).

The two claims show that \(A(p) = B(p)\) if and only if \(p \equiv 1 \text{ mod } 4\).