PSet 9 Solutions

(1) Notice that gnome d will flip switch n if and only if $d | n$. 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 $1, 4, 9, 16, 25, \dots$, 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 $d = n/d$, ie. $d = \sqrt{n}$ (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 $\sqrt{n} \in \mathbb{Z}$ (ie. 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 $\boxed{31}$ 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

$$s^{ef} \equiv s \bmod m \iff \text{both } s^{ef} \equiv s \bmod p \text{ and } s^{ef} \equiv s \bmod q.$$

Now, $ef \equiv 1 \bmod \varphi(m)$ and $\varphi(m) = (p-1)(q-1)$, so $ef \equiv 1 \bmod (p-1)$ as well. This implies, by Fermat's little theorem, that

$$\underline{\text{if}} \quad \gcd(s,p) = 1, \quad \underline{\text{then}} \quad s^{ef} \equiv s \bmod p.$$

However, it is also possible that $\gcd(s,p) \neq 1$. Since p is prime, this can only be true if $p | s$, ie. $s \equiv 0 \bmod p$. But in this case,

$$s^{ef} \equiv 0^{ef} \equiv 0 \equiv s \bmod p.$$

So in either case (whether $p | s$ or not), $s^{ef} \equiv s \bmod p$.

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

Therefore for all s, s^{ef} & s are congruent mod p & mod 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 $e = f = 5$ then indeed $ef = 25 \equiv 1 \bmod \varphi(45)$.

However, consider $s = 3$. Then

$$
\begin{aligned}
s^1 &\equiv 3 \bmod 45 \\
s^2 &\equiv 9 \bmod 45 \\
s^3 &\equiv 27 \bmod 45 \\
s^6 &\equiv 27^2 \equiv 729 \equiv 9 \bmod 45 \\
s^{12} &\equiv 81 \equiv -9 \bmod 45 \\
s^{24} &\equiv (-9)^2 \equiv 81 \equiv -9 \bmod 45 \\
s^{25} &\equiv -9 \cdot 3 \equiv -27 \equiv 18 \bmod 45
\end{aligned}
$$

So $s^{ef} \equiv 18$, while $s \equiv 3 \pmod{45}$. So f 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 $s^{ef} \equiv s \bmod 5$, 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 $s^f \% m$. Then

$$t^e \equiv (s^f)^e \equiv s^{fe} \equiv s \bmod m, \text{ as desired.}$$

b) Computing t from s amounts to solving

$$x^e \equiv s \bmod m \quad \text{for } x.$$

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 $\{1, 2, \cdots, p-1\}$ and reduce.

* $p=2$: QRs: $1 \bmod 2$
  NRs: none.

$p=3$: QRs: $1 \bmod 3$
NRs: $2 \bmod 3$.

$p=5$: QRs: $1, 4 \bmod 5$
NRs: $2, 3 \bmod 5$

$p=7$: squares $1, 4, 9$ reduce to $1, 4, 2$.

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) $A(2) = 1$ $B(2) = 0$
$A(3) = 1$ $B(3) = 2$
$A(5) = 5$ $B(5) = 5$ $\longleftarrow$
$A(7) = 7$ $B(7) = 14$
$A(11) = 22$ $B(11) = 33$
$A(13) = 39$ $B(13) = 39$ $\longleftarrow$
$A(17) = 68$ $B(17) = 68$ $\longleftarrow$
$A(19) = 76$ $B(19) = 95$

c) It appears that $A(p) = B(p)$ when $p \equiv 1 \bmod 4$. Indeed this is the case for all p. Here is a proof (not part of the homework since it uses material from Fridays class):

Claim 1: If $p \equiv 3 \bmod 4$ (or $p=2$) then $A(p) \neq B(p)$.
Pf: Note $A(p) + B(p) = 1 + 2 + 3 + \cdots + (p-1) = \frac{p(p-1)}{2}$ (sum of an arithmetic series) and $p(p-1) \equiv 2 \bmod 4$, so $A(p)+B(p)$ is odd. Thus its impossible ~~to~~ for $A(p)$ to equal $B(p)$.

Claim 2: If $p \equiv 1 \bmod 4$, then $A(p) = B(p)$.
Pf. If $p \equiv 1 \bmod 4$, then $\left(\frac{-1}{p}\right) = 1$, ie. ~~-1 is a~~ $p-1$ is a QR mod p. So for all a,

$$a \text{ is a QR} \iff p-a \text{ is a QR.}$$

So the QRs are paired off into pairs summing to p. This means the sum of all of them is $(\#\text{QRs}) \cdot \frac{p}{2}$. The same is true of the NRs. So both sums $A(p)$ & $B(p)$ are equal to $\frac{1}{4}(p-1) \cdot p$.

The two claims show that $A(p) = B(p)$ if and only if $p \equiv 1 \bmod 4$.

gnome	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
3	1	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0	1
4	1	0	0	1	1	1	1	1	0	0	1	0	1	0	0	1	1	1	1	1	0	0	1	0	1	0	0	1	1	1	1	1	0	0	1	0	1	0	0	1	1
5	1	0	0	1	0	1	1	1	0	1	1	0	1	0	1	1	1	1	1	0	0	0	1	0	0	0	0	1	1	0	1	1	0	0	0	0	1	0	0	0	1
6	1	0	0	1	0	0	1	1	0	1	1	1	1	0	1	1	1	0	1	0	0	0	1	1	0	0	0	1	1	1	1	1	0	0	0	1	1	0	0	0	1
7	1	0	0	1	0	0	0	1	0	1	1	1	1	1	1	1	1	0	1	0	1	0	1	1	0	0	0	0	1	1	1	1	0	0	1	1	1	0	0	0	1
8	1	0	0	1	0	0	0	0	0	1	1	1	1	1	1	0	1	0	1	0	1	0	1	0	0	0	0	0	1	1	1	0	0	0	1	1	1	0	0	1	1
9	1	0	0	1	0	0	0	0	1	1	1	1	1	1	1	0	1	1	1	0	1	0	1	0	0	0	1	0	1	1	1	0	0	0	1	0	1	0	0	1	1
10	1	0	0	1	0	0	0	0	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	0	0	0	1	0	1	0	1	0	0	0	1	0	1	0	0	0	1
11	1	0	0	1	0	0	0	0	1	0	0	1	1	1	1	0	1	1	1	1	1	1	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1
12	1	0	0	1	0	0	0	0	1	0	0	0	1	1	1	0	1	1	1	1	1	1	1	1	0	0	1	0	1	0	1	0	1	0	1	1	1	0	0	0	1
13	1	0	0	1	0	0	0	0	1	0	0	0	0	1	1	0	1	1	1	1	1	1	1	1	0	1	1	0	1	0	1	0	1	0	1	1	1	0	1	0	1
14	1	0	0	1	0	0	0	0	1	0	0	0	0	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	0	1	0	1	0	1	1	1	0	1	0	1
15	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	0	1	1	1	0	1	0	1
16	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	1	0	1
17	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1
18	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1	0	1	0	1
19	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	0	1
20	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1
21	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1
22	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1
23	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1
24	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1
25	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1
26	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1
27	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1	0	1	1	1	1	1
28	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	0	1	1	1	1	1
29	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	0	1	1	1	1	1
30	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	1	1	1	0	1	1	1	1	1
31	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	1	0	1	1	1	1	1