Q1 (a). First we compute $r = 12^9 \pmod{67}$.

$$12^2 \equiv 144 \pmod{67}$$
$$\equiv 10 \pmod{67}$$
$$12^4 \equiv 10^2 \equiv 100 \equiv 33 \pmod{67}$$
$$12^8 \equiv 33^2 \equiv 1089 \equiv 17 \pmod{67}$$
$$12^9 = 12 \cdot 12^8 \equiv 12 \cdot 17 = 204 \equiv 3 \pmod{67}$$

Then we compute $t = 8 \cdot 34^9 \pmod{67}$.

$$8 \cdot 34^9 \equiv 8\left(\frac{1}{2}\right)^9 \pmod{67}$$
$$\equiv \frac{1}{2^6} \pmod{67}$$
$$\equiv \frac{1}{64} \pmod{67}$$
$$\equiv (-3)^{-1} \pmod{67}$$
$$= 22 \pmod{67}.$$

So the encryption of 8 is $(3, 22)$.

(b) To decrypt, Homer computes $tr^{-a} \pmod{p}$ where a is his secret key, ie

$$22 \cdot 3^{-37} \pmod{67}.$$

This can be done quickly using a repeated squaring algorithm to compute $3^{37} \pmod{67}$

Q2 (a): $50x + 271 \equiv 101 \pmod{502}$

$\iff 50x \equiv -160 \pmod{502}$

$\iff 25x \equiv -80 \pmod{251}$.

Since $\gcd(25, 251) = 1$, this has a unique solution mod 251.

∴ There is 1 solution mod 251 (or 2 solution mod 502).

(b). By Fermat's little theorem, for all $a \not\equiv 0 \pmod{73}$, we have $a^{72} \equiv 1 \pmod{73}$ which implies $a^{144} \equiv (a^{72})^2 \equiv 1^2 \equiv 1 \pmod{73}$.

Thus we have found 72 solutions mod 73 to the congruence $x^{144} \equiv 1 \pmod{73}$.

Since $x = 0$ is clearly not a solution, there are exactly 72 solutions mod 73

(c) $303 = 3 \times 101$ with 3 and 101 both prime.

We solve: $x^2 \equiv 9 \pmod{3}$ which has the one solution $x \equiv 0 \pmod{3}$.

We solve $x^2 \equiv 9 \pmod{101}$:

ie $(x-3)(x+3) \equiv 0 \mod 101$

ie $x \equiv \pm 3 \pmod{101}$ as 101 is prime.

By the Chinese remainder theorem, each combination of a mod 3 solution and a mod 101 solution yields a mod 303 solution.

∴ There are $1 \times 2 = 2$ solutions mod 303.

(d). $\gcd(57, 499) = \gcd(57, 9 \times 57 - 499)$

$= \gcd(57, 514)$

$= \gcd(3 \times 19, 2 \times 7)$

$= 1$.

∴ By the Chinese remainder theorem, there exists a unique solution modulo $59 \times 499 = 29441$.

Q3 (a) We prove by induction on d that the algorithm $P(y, a, d, n)$:

While $d \neq 0$
- If d is even: $a = a^2 \pmod n$, $d = d/2$
- If d is odd: $y = ay \pmod n$, $a = a^2 \pmod n$, $d = \frac{d-1}{2}$

Return y

computes the value $ya^d \pmod n$.

The $d = 0$ case is trivial, so assume $d \geq 1$.

If d is even, after one step we run the algorithm

$$P(y, a^2, \tfrac{d}{2}, n).$$

Since $d/2 < d$, by inductive assumption we compute $y(a^2)^{d/2} \pmod n$ which is the same as $ya^d \pmod n$ as required.

If d is odd, after one step we run the algorithm

$$P(ay, a^2, \tfrac{d-1}{2}, n).$$

Since $0 \leq \frac{d-1}{2} < d$, by inductive assumption we compute

$$(ay) \cdot (a^2)^{\frac{d-1}{2}} \pmod n, \text{ which is the same as}$$

$$ya^d \pmod n, \text{ as required.}$$

(b) At each execution of the while loop, the number of binary digits of d decreases, so the while loop is executed $O(\log d)$ times.

The arithmetic operations of multiplication modulo n can be computed in $O((\log n)^2)$ time so overall the runtime of the algorithm is $O\left((\log d) \cdot (\log n)^2\right)$.

Note: Any reasonable understanding that there was some time cost to computing the multiplications was sufficient for full marks here

Q4 (a)

$$b \equiv 1 \pmod{b-1}$$

$$\therefore b^4+b^3+b^2+b^1+1 \equiv 1^4+1^3+1^2+1^1+1 \equiv 5 \pmod{b-1}.$$

$$\therefore \gcd(b-1,\ b^4+b^3+b^2+b+1) \mid 5 \quad (*)$$

If $b \equiv 1 \bmod 5$ then $5 \mid b-1$ and

$$b^4+b^3+b^2+b^1+1 \equiv 1^4+1^3+1^2+1+1 \pmod 5$$
$$\equiv 0 \pmod 5$$

so in this case $\gcd(b-1, b^4+b^3+b^2+b+1) = 5$.

If $b \not\equiv 1 \bmod 5$ then $5 \nmid b-1$ so using $(*)$, it must be that $\gcd(b-1, b^4+b^3+b^2+b+1) = 1$, as required.

(b) Since $p \mid b^4+b^3+b^2+b+1$, $p \mid b^5-1$ as $b^5-1 = (b-1)(b^4+b^3+b^2+b+1)$.

$$\therefore b^5 \equiv 1 \pmod p.$$

$$\therefore \operatorname{ord}_p(b) \mid 5.$$

So either $\operatorname{ord}_p(b) = 1$ or $\operatorname{ord}_p(b) = 5$.

If $\operatorname{ord}_p(b) = 1$ then $p \mid b-1$ and hence $p \mid \gcd(b-1, b^4+b^3+b^2+b+1)$.

By part (a), this implies $p \mid 5$. As $p \neq 5$ is given this is a contradiction.

$$\therefore \operatorname{ord}_p(b) = 5.$$

By Fermat's Little theorem, $b^{p-1} \equiv 1 \pmod p$.

$$\therefore \operatorname{ord}_p(b) \mid p-1$$

ie $5 \mid p-1$

ie $p \equiv 1 \pmod 5$.