35) a) Addition: 1 addition for each digit plus possibly one carry: $3n$ operations, $\mathcal{O}(n)$

b) There is multiplication of any pair of digits: n^2 digit multiplications, respectively addition of n numbers of n digits: $O(n^2)$ operations.

36) a) For the order of r^e to be 2, we need that $\frac{p-1}{\gcd(p-1,e)} = 2$, i.e. $\gcd(p-1,e) = \frac{p-1}{2}$. This is ($p$ is odd!) only possible for $e = \frac{p-1}{2}$

b) We need that $k = \frac{p-1}{\gcd(p-1,e)}$, so $\gcd(p-1,e) = \frac{p-1}{k}$

This means that $e = \frac{p-1}{k} \cdot a$, where $\gcd(a,k) = 1$ and

$a < k$ (as otherwise $r^e \equiv \underbrace{\left(r^{\frac{p-1}{k}}\right)}_{\text{order } k}{}^{a} \equiv \left(r^{\left(\frac{p-1}{k}\right)}\right)^{a \bmod k}$

There are exactly $\varphi(k)$

such a's.

37 a) $\mathrm{OrderMod}_p(x) = \dfrac{p-1}{\gcd(p-1,a)} = \dfrac{ab}{\gcd(ab,a)} = b$, ditto $\mathrm{OrderMod}_p(y) = a$.

b) We know that $\mathrm{OrderMod}_p(x^e)$ divides b, as $\gcd(a,b)=1$ the only way that $x^e = y^f$ is that $\mathrm{OrderMod}_p(x^e) = 1$, so $x^e = 1$

c) As $1 = \gcd(a,b)$ there ex. u, v s.t. $1 = ua + vb$

Then $r = r^1 = r^{ua+vb} = (r^a)^u (r^b)^v = x^u y^v$.

(Note: As x^a has finite order we can add multiples of $\mathrm{OrderMod}_p(x)$ to u to make it nonnegative. Ditto v nonnegative. But then if $z = r^d$ then

$z = r^d = (x^u y^v)^d = x^{(ud)} y^{(vd)}$, so set $e = ud$, $y = vd$.

d) $1 = 31 \cdot 10 - 3 \cdot 103$, so $g = (g^{10})^{31} \cdot (g^{103})^{-3} =$ Order 10 equivalent to 7

$(g^{10})^{31} (g^{103})^7$. So $2 \equiv g^{796} = (g^{10})^{\underbrace{24676}_{e\,\equiv\,59\,(103)}} (g^{103})^{\underbrace{5572}_{f\,\equiv\,2\,(10)}}$

39) If gcd$(a, p-1)$ is large, then the order of g^a is small. An attacker can detect this. But as there are just $\varphi(n)$ elements of order n, and $n \mid$ (and thus $\varphi(n)$) is small. Thus the attacker could determine a.

38) Was too hard - apologies.