① a)

To check whether a is a square or not in F_p^* (in polynomial time) we can use the Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ -1 & \text{if } a \text{ is a non-square modulo } p \\ 1 & \text{if } a \text{ is a square modulo } p \end{cases}$$

We have

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$$

$-1 \mod p$ is $p-1$, so we have:

if $a^{(p-1)/2} = 1 \mod p$, a is a square mod p
if $a^{(p-1)/2} = p-1 \mod p$, a is not a square mod p

Since we can do modular esxponentiation in $O(\log n)$, we can find whether a is a square or not in polynomial time.

① b) Given: $p \equiv 3 \bmod 4$, a - square in F_p^*

Prove: $a^{\frac{(p+1)}{4}}$ is a square root of a

Proof:

Since $p \equiv 3 \bmod 4$, it is guaranteed that $\frac{p+1}{4}$ is an integer, so a is raised to an integer power

In order for $a^{\frac{p+1}{4}}$ to be a square root of a in F_p, we must have:

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv a \bmod p$$

Expanding the left side, we have:

$$\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{\cancel{4}\,2}\cdot\cancel{2}} = a^{\frac{p+1}{2}}$$

We can rewrite this as:

$$a^{\frac{p-1+2}{2}} = a^{\frac{p-1}{2}} \cdot a^{\frac{2}{2}} = a^{\frac{p-1}{2}} \cdot a$$

As a is a square in F_p^*, the Legendre symbol satisfies:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$$

where $\left(\frac{a}{p}\right) = 1$

We can therefore substitute $a^{\frac{p-1}{2}}$ with 1, so at the end we have:

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv 1 \cdot a \bmod p$$

So $a^{\frac{p+1}{4}}$ is indeed a square root of a, given $p \equiv 3 \bmod 4$

① c) Probability of r being not a ~~non~~ square mod p:

To know the probability, we must first find how many non-squares there are in $\mathbb{F}_p^*$

For r to be a non-square modulo p, we must have a Legendre symbol:

$$\left(\frac{r}{p}\right) = -1$$

We know that, taking ~~x and y~~ $x, y \in \mathbb{F}_p^*$, s.t. $x^2 \equiv y^2$

$$x^2 \equiv y^2 \iff x \equiv \pm y \mod p$$

So, the set $\left\{1^2, 2^2, \ldots \left(\frac{p-1}{2}\right)^2\right\}$ must be the set of all non-zero quadratic residues. We therefore have $\frac{p-1}{2}$ quadratic residues (excluding 0) and $\frac{p-1}{2}$ quadratic non-residues.

As p nears infinity, the probability of r being a non-square mod p is

$$\lim_{p\to\infty} P\left(\left(\frac{r}{p}\right) = -1\right) = \lim_{p\to\infty} \frac{\frac{p-1}{2}}{p} = \lim_{p\to\infty} \frac{p-1}{2p} = \lim_{p\to\infty}\left(\frac{\cancel{p}^1}{2\cancel{p}} - \frac{1}{2p}\right) =$$

$$= \lim_{p\to\infty}\left(\frac{1}{2} - \frac{1}{2p}\right) = \frac{1}{2}$$

So, the probability of r being a non-square mod p is $\frac{1}{2}$.

① c) Prove: Tonelli-Shanks algorithm terminates and returns a square root of a

Proof: In the initial state, we have:

$\left(\frac{a}{p}\right) = 1$

$p-1 = 2^S Q$, $Q \equiv 1 \bmod 2$, $r \in \mathbb{F}_p^*$

$w = a^{\frac{Q+1}{2}}$ $\qquad \left(\frac{r}{p}\right) = -1$

$j = 1$ $\qquad y = r^Q$

$a' = a^{-1} \bmod p$

And we need to find w s.t.

$$w^2 = a \bmod p$$

$i = j = 0$

For the algorithm to terminate, we must find $\sqrt{(w^2 a')^{2^i}}$ at some iteration, such that $(w^2 a')^{2} = 1 \pmod p$, updating $w = w y^{2^{S-i-1}}$

If $(w^2 a')^{2^0} \neq 1 \bmod p$, we consider the aforementioned r. or rather, the transformation we make to it - y. We have

$y^{2^S} \equiv (r^Q)^{2^S} \equiv r^{Q 2^S} \equiv r^{p-1} \equiv 1 \bmod p$, and in a similar way, $y^{2^{S-1}} \equiv r^{\frac{p-1}{2}} \equiv -1 \bmod p$, hence $\operatorname{ord}(y) = 2^S$

We have $(w^2 a')^{2^S} \equiv 1 \bmod p$, so $\operatorname{ord}(w^2 a') \mid 2^S$. If we take the order of $w^2 a'$ to be 2^i, since a is a square modulo p, $i < S-1$

~~When~~ ~~takin~~ In the loop, when taking $w = w y^{2^{S-i-1}}$, $y^{2^{S-i-1}}$ should therefore have an order 2^{i-1}. This means that the new w has order 2^s with $s < i$

If $i=0$ then $w^2 a^1 \equiv 1 \mod p$, the algorithm ~~terminates~~ stops, and returns w. In any other case, the loop will continue, untill we arrive at such value. And since the sequence of S is decreasing, the algorithm will terminate (at some point)

① d) Given: Algorithm, solving square roots in F_p^* for $\forall$ prime p

square-free integer n, $n = pq$, $p \neq q$

Prove: (probabilistic) finding square roots modulo $n \iff$ (probabilistic) factoring n

Proof: Assume that the algorithm returns r - a non-trivial square root modulo n. Then, r has the following properties:

$$r^2 = 1 \mod n$$
$$r + 1 \neq 0 \mod n$$
$$r - 1 \neq 0 \mod n$$

and also $r \neq \pm 1 \mod n$.

We therefore have

$$r^2 - 1 = 0 \mod n$$

which, rewritten in canonical form

$$r^2 - 1 = 0 + kn \text{ for some } k \in \mathbb{Z}$$

taking the left side as a difference of two squares, we have:

$$(r-1)(r+1) = kn$$

So, if we take $\gcd(r-1, n)$ and $\gcd(r+1, n)$, one of them must be larger than 1, otherwise the equality above will fail.

However, if gcd of one of them differs from 1, this means that (as $n = pq$) p and q must divide one of $r-1$ or $r+1$. Hence, if ~~we can find an algorithm~~ there is a (probabilistic) algorithm to find square roots modulo n, it is equivalent to a (probabilistic) algorithm to factor n