14. Composite

It is interesting to see how to relate the problem of being a quadratic residue modulo $m$ to being a quadratic residue modulo a prime.

**Theorem 14.1.** Let $m$ be a natural number bigger than one and let $a$ be coprime to $m$.

Then $a$ is a quadratic residue of $m$ if and only if $a$ is a quadratic residue of every odd prime dividing $m$ and either $m$ is not divisible by 4, or $m$ is divisible by 4 but not 8 and $a$ is congruent to one modulo 4, or $m$ is divisible by 8 and $a$ is congruent to one modulo 8.

**Proof.** Let $m = 2^e p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ be the prime factorisation of $m$. We want to solve the equation

$$x^2 \equiv a \mod m.$$

By the Chinese remainder theorem it is enough to solve the equation for every prime $p$ dividing $m$.

First suppose that $p$ is an odd prime. Certainly if $a$ is quadratic residue modulo $p^e$ then it is a quadratic residue modulo $p$. For the reverse direction consider the polynomial $f(x) = x^2 - a$. If $x_0$ is a root then $x_0 \not\equiv 0 \mod p$. $f'(x) = 2x$ so that $f'(x_0) = 2x_0 \not\equiv 0 \mod p$. Thus $x_0$ is non-singular and general theory says we can lift $x_0$ uniquely to a solution modulo $p^e$, for any $e$.

Now suppose that $p = 2$. Note that 1 is a quadratic residue modulo 2 and so there is no condition if $e = 1$. If $e = 2$ then note that 1 is the only non-zero quadratic residues modulo 4, so that $a \equiv 1 \mod 4$. If $e \geq 3$ then it is proved in Chapter 4 that the only quadratic residues are congruent to one modulo 8. \qed

In fact one can push this analysis a bit further and find the number of solutions to the equation $x^2 \equiv a \mod m$.

**Theorem 14.2.** Suppose that $m > 1$ and that $a \in U_m$ is a unit.

If the equation $x^2 \equiv a \mod m$ has a solution then it has $2^r + u$ solutions, where $r$ is then number of odd distinct prime factors of $m$ and

$$u = \begin{cases} 
0 & \text{if 4 does not divide } m \\
1 & \text{if 4 divides } m \text{ but not 8} \\
2 & \text{if 8 divides } m.
\end{cases}$$

**Proof.** We apply the Chinese remainder theorem. Suppose $p$ is an odd prime dividing $m$. By assumption the polynomial $x^2 - a$ has a root modulo $p$. If $b$ is a root then so is $-b \not\equiv b \mod p$. As $\mathbb{Z}_p$ is a field the polynomial $x^2 - a$ has at most two roots. Therefore it has exactly two
roots. As both roots are non-singular, as in the proof of (14.1) we can lift both solutions to unique solutions modulo $p^e$.

Now suppose that $p = 2$ divides $m$. If 4 does not divide $m$ then $a \equiv 1 \mod 2$ and $x^2 \equiv a \mod 2$ has one solution, $x_0 = 1$. If 4 divides $m$ but not 8 then $a \equiv 1 \mod 4$ and there are $2 = 2^1$ solutions, 1 and 3, to the equation $x^2 \equiv 1 \mod 4$. If 8 divides $m$ then it is proved in Chapter 4 that there are $4 = 2^2$ solutions. □