Some questions about $\mathbb{Z}[\sqrt{-5}]$:

1. Which $\mathbb{Z}$-primes p remain prime in $\mathbb{Z}[\sqrt{-5}]$?

2. Which $\mathbb{Z}$-primes p are irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$?

3. Which $a + b\sqrt{-5}$ $(b \neq 0)$ are prime in $\mathbb{Z}[\sqrt{-5}]$?

4. Which $a + b\sqrt{-5}$ $(b \neq 0)$ are irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$?

The following facts, conjectured by Euler and proved by Lagrange, are needed.

Let p be an odd $\mathbb{Z}$-prime $\neq 5$. Then:

• $p = a^2 + 5b^2$ $(a, b \in \mathbb{Z})$ if (hard) and only if (easy) $p = 20n + 1$ or $p = 20n + 9$ for some $n \in \mathbb{Z}$.

• $2p = a^2 + 5b^2$ $(a, b \in \mathbb{Z})$ if (hard) and only if (easy) $p = 20n + 3$ or $p = 20n + 7$ for some $n \in \mathbb{Z}$.

(You might check that these statements are true for some small primes.)

Now here are some answers to questions 1–3. p will always be a $\mathbb{Z}$-prime.

• *p is reducible* in $\mathbb{Z}[\sqrt{-5}]$ if and only if $p = a^2 + 5b^2$ for some a, b in $\mathbb{Z}$—that is, if and only if $p = 20n + 1$ or $p = 20n + 9$ for some $n \in \mathbb{Z}$.

Proof. Since $a^2+5b^2 = (a+b\sqrt{-5})(a-b\sqrt{-5})$, and both factors have norm a^2+5b^2, therefore any integer > 1 of the form $a^2 + 5b^2$ is reducible in $\mathbb{Z}[\sqrt{-5}]$.

Conversely, if p is reducible, say $p = \alpha\beta$ (both factors having norm > 1), then $p^2 = N(p) = N(\alpha)N(\beta)$ (where N denotes "norm"), and therefore $N\alpha$ (which can't be 1 or p^2, since $N(\beta) > 1$) must be p. So if $\alpha = a + b\sqrt{-5}$ then $p = a^2 + 5b^2$. □

• Suppose $2p = a^2 + 5b^2$ for some a, b in $\mathbb{Z}$—that is, $p = 20n + 3$ or $p = 20n + 7$ for some $n \in \mathbb{Z}$. Then a and b can't both be divisible by p, since $2p$ is not divisible by p^2. So p divides neither of $a \pm b\sqrt{-5}$, whereas it does divide their product; thus *p is not prime* in $\mathbb{Z}[\sqrt{-5}]$. Moreover, *p is irreducible* in $\mathbb{Z}[\sqrt{-5}]$, because otherwise we'd have $p = c^2 + 5d^2$, and then both p and $2p$ would be $\equiv 1$ or $4 \pmod 5$.

• The other possible remainders when p is divided by 20 are 11, 13, 17, or 19. It can be shown, using the *quadratic reciprocity theorem* (google it!) that when one of these remainders occurs, then *p is prime* in $\mathbb{Z}[\sqrt{-5}]$.

For large integers N, approximately half the primes $< N$ behave this way—google "Dirichlet arithmetic progression".

• If $a + b\sqrt{-5}$ $(b \neq 0)$ is prime in $\mathbb{Z}[\sqrt{-5}]$, then its norm $a^2 + 5b^2$ is prime in $\mathbb{Z}$.

Proof. Since $a + b\sqrt{-5}$ is prime, and it divides $a^2 + 5b^2$, therefore it divides some $\mathbb{Z}$-prime factor q of $a^2 + 5b^2$, say $(a + b\sqrt{-5})\beta = q$, where $\beta \neq \pm 1$ because $b \neq 0$. Then

$$(a^2 + 5b^2)N(\beta) = N(a + b\sqrt{-5})N(\beta) = N(q) = q^2,$$

and since $N(\beta) > 1$ therefore $a^2 + 5b^2 = N(a + b\sqrt{-5}) = q$. □

Conversely, if $a^2 + 5b^2 \neq 5$ is prime in $\mathbb{Z}$ then $a + b\sqrt{-5}$ is prime in . We'll show this later; but meanwhile it's clear that $a + b\sqrt{-5}$ is at least irreducible.

Thus finding the primes of the form $a+b\sqrt{-5}$ $(ab \neq 0)$ is the same as determining all relations of the form $q = a^2 + 5b^2$ with $ab \neq 0$ and q a $\mathbb{Z}$-prime.

For example, $89 = 3^2 + 5 \cdot 4^2$, so $3 \pm 4\sqrt{-5}$ are both prime in $\mathbb{Z}[\sqrt{-5}]$.

Conclusion. Questions 1–4 lead to questions about ordinary integers that played an important historical role in the development of number theory (but were not originally thought of in connection with $\mathbb{Z}[\sqrt{-5}]$).

For more in this vein, and its vast implications, see, e.g. the book "Primes of the form x^2+ny^2" by David Cox. <http://www.cs.amherst.edu/~dac/primes.html>