1. Classify the Primes in $\mathbb{Z}[\sqrt{2}]$

Ingredient: the norm map $N(a + b\sqrt{2}) = a^2 - 2b^2$ and maybe some Frobenius reciprocity which I’ll explain later.

- **Suppose that $x \in \mathbb{Z}[\sqrt{2}]$ were a prime element.** That is to say, whenever $x | ab$ it implies that either $x | a$ or $x | b$.
- Then $N(x) = N(x_1 + \sqrt{2}x_2) = \pm (x_1 + \sqrt{2}x_2)(x_1 - \sqrt{2}x_2) = p_1p_2\ldots p_n$ where the $p_i$ form the unique factorization of $N(x)$ in $\mathbb{Z}$. (They aren’t necessarily distinct)
- Since $x_1 + \sqrt{2}x_2$ is prime, and it divides the product $p_1p_2\ldots p_n$, it must divide one of the $p_i$. In other words $x \cdot z = p_i$ for some $z \in \mathbb{Z}[\sqrt{2}]$.
- Therefore, taking the norm of that relationship $N(x \cdot z) = N(p_i)$ we have that $N(x)N(z) = p_i^2$. And therefore $p_1p_2\ldots p_nN(z) = p_i^2$ in $\mathbb{Z}$.
- By unique factorization in $\mathbb{Z}$ we have that $N(x)$ is either $p_i$ or $p_i^2$ where $p_i$ is a prime in $\mathbb{Z}$.

This is a necessary condition for $x$ to be a prime element in $\mathbb{Z}[\sqrt{2}]$. Now we want to find sufficient conditions

- Suppose $N(a + \sqrt{2}b) = p$ where $p$ is a prime in $\mathbb{Z}$ then $a + \sqrt{2}b$ is prime in $\mathbb{Z}[\sqrt{2}]$ most of you showed this.
- Now suppose that $N(a + \sqrt{2}b) = p^2$. This breaks into two cases.

**Case 1.** Suppose $p$ is a prime in $\mathbb{Z}[\sqrt{2}]$ and in $\mathbb{Z}$.

- Then since $p^2 = \pm(a + \sqrt{2}b)(a - \sqrt{2}b)$, since we’re in a unique factorization domain, $a + \sqrt{2}b$ is an associate to $p$.

**Case 2.** Suppose that $p$ isn’t prime in $\mathbb{Z}[\sqrt{2}]$.

- Suppose (by contradiction) that $x = a + \sqrt{2}b$ is a prime element. Then, $(a + \sqrt{2}b)p^2 \implies (a + \sqrt{2}b)p \implies (a + \sqrt{2}b) \cdot z_1 = p$.
- We could do a similar thing with $\bar{x} = a - \sqrt{2}b$ so that $(a - \sqrt{2}b) \cdot z_2 = p$. (you have to use the easy fact that $x$ is prime $\iff \bar{x}$ is prime)
- Combining the above two points we have that $p^2 = \pm z_1 z_2 (a - \sqrt{2}b)(a + \sqrt{2}b)$ but, on the other hand, $p^2 = \pm (a - \sqrt{2}b)(a + \sqrt{2}b)$ so $z_1$ and $z_2$ are units.
- Therefore $x$ is associate to $p$ which we supposed was not a prime in $\mathbb{Z}[\sqrt{2}]$ so $x$ is not prime.

Therefore, a sufficient condition for $x$ to be prime is either $N(x) = p$ or $N(x) = p^2$ where $p$ is a prime in $\mathbb{Z}$ and $\mathbb{Z}[\sqrt{2}]$.

In summary, $x$ is a prime in $\mathbb{Z}[\sqrt{2}]$ if and only if one of the following is true:

- $N(x) = p$ where $p$ is a prime in $\mathbb{Z}$.
- $N(x) = p^2$ where $p$ is a prime in $\mathbb{Z}$ that remains prime in $\mathbb{Z}[\sqrt{2}]$.

All that remains is to find the primes $p$ which are primes in both $\mathbb{Z}$ and $\mathbb{Z}[\sqrt{2}]$. In other words, which primes in $\mathbb{Z}$ remain prime when we extend to $\mathbb{Z}[\sqrt{2}]$. You can do this with quadratic reciprocity. The basic theorem tells you that $p$ is NOT prime if and only if $p \equiv \pm 1 \mod 8$.

2. Finding non-trivial solutions to $a^2 - db^2 = 1$

**Lemma.** Let $d$ be a square free integer, then for infinitely many pairs of integers $P_N, Q_N$
Most of you showed this easily. The proof involves the pigeonhole principal (yay!).

Now, take the relationship $|\sqrt{d} - \frac{P_N}{Q_N}| < \frac{1}{Q_N^2}$ and multiply both sides by $Q_N(\sqrt{d}Q_N + P_N)$. We get that

$$|dQ_N^2 - P_N^2| < \sqrt{d} + \frac{P_N}{Q_N} < 2\sqrt{d} + 1$$

Where the second “<” follows from that fact that $|\sqrt{d} - \frac{P_N}{Q_N}| < 1 \implies -1 < \sqrt{d} - \frac{P_N}{Q_N}$.

Now, there are only finitely many integers less than $2\sqrt{d} + 1$, but infinitely pairs $(Q_N, P_N)$ such that $|dQ_N^2 - P_N^2| < 2\sqrt{d} + 1$. So in order to fit an infinite number of pairs into a finite number of boxes, an infinite number of pairs have to go to the same thing, say $n$, which, remember is less than $2\sqrt{d} + 1$.

So now, let's restrict ourselves to the infinite set of pairs $(Q_N, P_N)$ such that $|dQ_N^2 - P_N^2| = n$.

Of this infinite set of pairs, there must be an infinite subset such that $Q_i \equiv Q_j \pmod{n}$. This is again the pigeonhole principal. There are an infinite number of $Q_N$ but only a finite number of congruences $\pmod{n}$.

Okay, so now restrict to the infinite set of pairs $(Q_N, P_N)$ where all the $Q_N$ are congruent to each other $\pmod{n}$. We can do the same thing again, and of these pairs find an infinite subset where, in addition $P_i \equiv P_j \pmod{n}$.

Now we have an infinite set of pairs $(Q_N, P_N)$ satisfying

1. $|dQ_N^2 - P_N^2| = n$
2. $Q_i \equiv Q_j \pmod{n}$
3. $P_i \equiv P_j \pmod{n}$.

For any two these pairs, let $A = P_i + Q_i\sqrt{d}$ and $B = P_j + Q_j\sqrt{d}$. Now there's just a lot of algebra to show that $\frac{A}{B} \in \mathbb{Z}[\sqrt{d}]$ and that $N\left(\frac{A}{B}\right) = 1$. I'll leave that to you.