(1) The most common mistake was in only performing one step of the algorithm. The base case of the algorithm is when $\deg(f) > \deg(g)$, whence we take $q = 0$ and $r = g$. Suppose then that $\deg(f) \leq \deg(g)$. Let $\deg(f) = m$ and $\deg(g) = n$. Also, let a be the leading coefficient of f, which we suppose to be a unit, and let b be the leading coefficient of g. The correct first step was to consider $q_0 = \frac{b}{a}t^{n-m}$ and $r_0 = g - fq_0$. Then by construction, $\deg(r_0) < \deg(g)$ and $g = fq_0 + r_0$.

It was common for people to end the construction here, but this in general only ensures that $\deg(r_0) = \deg(g)-1$, which could still be way bigger than $\deg(f)$. For instance, take $g = x^{100}-1$ and $f = x - 1$. Then $q_0 = x^{99}$ and $r_0 = x^{99} - 1$, which is a much higher degree than f.

The correct continuation is to do this recursively. We have $g = fq_0 + r_0$, and we now repeat this procedure to write $r_0 = fq_1 + r_1$ and then $r_1 = fq_2 + r_2$, etc, with $\deg(r_i) < \deg(r_{i-1})$. Note that we are always dividing by f here, so the hypothesis that the leading coefficient of the denominator is a unit never changes. Plugging in bakcwards yields

$$g = (q_0 + \cdots + q_i)f + r_i$$

and this algorithm terminates to the base case eventually, as the degrees of the r_i are strictly decreasing natural numbers. Hence, this algorithm will yield our desired long division. This is exactly the polynomial long division algorithm taught in, say, algebra 2.

(2) The most common mistake was in assuming that the hypothesized euclidean function on $R[t]$ must be the degree function. One can prove that the degree function itself being a euclidean function implies that R is a field, but could there be some sneaky other function? The answer is no, but it's a priori a possibility.

In fact, a stronger statement is true - if $R[t]$ is a PID then R is a field. A slick proof some people gave was to consider the ideal (t). This is the kernel of the map $R[t] \longrightarrow R$ via $f \mapsto f(0)$, which is onto, so (t) is prime as R is assumed to be domain. If $R[t]$ was a PID then nonzero primes are maximal, so (t) is maximal. Thus, R is a field.

This argument lives in a general setting called dimension theory. Here's a bizarre definition (which maybe makes more sense if you think about R as the coordinate ring of a variety and try to draw some pictures).

Definition 0.1. Let R be a commutative ring. Its (Krull) dimension is

$$\sup\{n \mid \text{there is a chain } \mathfrak{p}_0 < \cdots < \mathfrak{p}_n \text{ of prime ideals in } R\}$$

For those who know set theory, n can range over the class of all ordinals rather than just $\mathbb{N}$. For instance, saying that $\dim(R) = 0$ means that all primes are maximal, so a field is a 0 dimensional domain. A PID which is not a field has dimension 1, as all its nonzero primes are maximal.

If R is Noetherian, $\dim R[x] = \dim R + 1$. Apparently (I have no clue why this is true) in general, if R is not Noetherian we can only conclude $\dim R + 1 \leq \dim R[x] \leq 2\dim R + 1$.

Try to consider some varieties X and compute $\dim \mathcal{O}(X)$. This sort of computation is hard in general, so maybe just write down a chain you believe to be of maximal length and convince yourself this notion of dimension aligns with your pictures.

My intuition for this problem was then that $R[x]$ being euclidean means it's one dimensional and Noetherian, so R would be a zero dimensional domain and hence a field. This is a very fancy way to say the proof above.

Another common method was to consider the ideal (a, x) for a a nonzero element of R and to consider what it means for this to be principal.

(3) (a) I'd like to present what I think is the cleanest approach. It was common to identity elements of $S^{-1}R$ with elements of $\mathbb{Q}[\sqrt{-d}]$. In the end, this is ok, but it must be rigorously justified via a morphism, as elements of $S^{-1}R$ are equivalence classes which a priori have no relation to elements of $\mathbb{Q}[\sqrt{-d}]$, even though they are written similarly. There is an inclusion map $\mathbb{Z}[\sqrt{-d}] \longrightarrow \mathbb{Q}[\sqrt{-d}]$. Furthermore, $\mathbb{Q}[\sqrt{-d}]$ is a field as given $\alpha \in \mathbb{Q}[\sqrt{-d}]$ we have that $\alpha^{-1} = \frac{\overline{\alpha}}{N(\alpha)}$, which is in $\mathbb{Q}[\sqrt{-d}]$. Hence, by universal property of the quotient, we have an induced map $S^{-1}R \longrightarrow \mathbb{Q}[\sqrt{-d}]$.

We know $S^{-1}R$ is a field, so its only ideals are (0) and (1). The kernel of $S^{-1}R \longrightarrow \mathbb{Q}[\sqrt{-d}]$ must be one of these, but the map is nonzero so the kernel is (0). Thus we are left to show surjectivity. But the image surely contains $\mathbb{Q}$ and $\sqrt{-d}$, so the map is onto.

(b) Not many mistakes here. Interestingly, the norm $N(\alpha)$ can be thought of as the determinant of the $\mathbb{Q}$-linear transformation $\mathbb{Q}(i) \longrightarrow \mathbb{Q}(i)$ sending $\beta \mapsto \alpha\beta$. This is a useful interpretation, and yields the multiplicativity desired due to multiplicativity of the determinant.

(c) The fundamental idea of setting the equation $a^2+db^2 = 1$ and using positivity of a^2, b^2, and d to rule out possbilities was commonly done, though there were occasional computational errors there (such as the case $d = 1$). This shows that for $d > 0$ we have that the unit group is finite. One can in fact show that the units are precisely the roots of unity in this case. However, for $d < 0$, the unit group is more complicated. It is known to be isomorphic to $\mathbb{Z} \times A$ for a cyclic group A (again, the group of roots of unity). See Dirichlet's unit theorem for more. There are some subtleties I'm brushing under the rug here, such as the issue of the "ring of integers" I mention in (4).

(d) A common issue was in not using the hypothesis $d \geq 3$. 2 is reducible in $\mathbb{Z}[\sqrt{-1}]$ as it factors as $(1 + i)^2$ up to units. It is also reducible in $\mathbb{Z}[\sqrt{-2}]$ as it factors as $(\sqrt{-2})^2$ up to units.

An interesting observation I'll make is that if $\pi \in \mathbb{Z}[i]$ is prime, we have that $|\mathbb{Z}[i]/(\pi)| = N(\pi)$, which will be either p or p^2 as it is a degree at most 2 field extension of $\mathbb{Z}/p\mathbb{Z}$, where $(p) = (\pi) \cap \mathbb{Z}$. I explain the last part a bit more in (8). As for why the norm is computed this way, I don't know a good elementary proof off hand, but this is a standard result in algebraic number theory textbooks.

(e) A common issue was not showing that 2 is not prime in these rings. This was common enough that I didn't take off points for it, but it is a useful thing to understand. If d is even, note that $2| - d = \sqrt{-d}^2$ but does not divide $\sqrt{-d}$ itself, as if $2 \mid a + b\sqrt{-d}$ then a and b would be even. If d is odd, $2|1 + d^2 = (1 + \sqrt{-d})(1 - \sqrt{-d})$ but it fails to divide both factors.

Another way to prove this is to compute the quotient $\mathbb{Z}[\sqrt{-d}]/(2)$. Indeed, this is isomorphic to

$$\mathbb{Z}[x]/(x^2 + d, 2)$$

which in turn is isomorphic to

$$\mathbb{Z}/2\mathbb{Z}[x]/(x^2 + d)$$

I explain this sort of computation in (8).

Now, every element of $\mathbb{Z}/2\mathbb{Z}$ is a square, so let $a^2 = d$ in $\mathbb{Z}/2\mathbb{Z}$. Then $x^2 + d = (x + a)^2$ in $\mathbb{Z}/2[x]/(x^2 + d)$, so this ring is not a domain and hence 2 is not prime in $\mathbb{Z}[\sqrt{-d}]$. This is essentially the same proof as the above.

(4) There weren't too many mistakes here, so I'll just make a few comments. First of all, this sort of norm won't always work. For instance, $\mathbb{Z}[\sqrt{-5}]$ has the norm $a+b\sqrt{-5} \mapsto a^2+5b^2$, but it's not Euclidean as it's not a UFD. There can also be domains of the form $\mathbb{Z}[\sqrt{d}]$ whose Euclidean functions do not arise from the field norm, such as $\mathbb{Z}[\sqrt{14}]$ which apparently has some horrid norm found here. There's a survey here about Euclidean norms in number theory. The relevant section would be about quadratic number fields.

Personally, I'm more interested in when such a ring is a PID than when it's Euclidean. By the way, $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is apparently a PID which is not Euclidean. See here. This is called the "class number 1" problem - as attached to these rings is a group called the class group, which measures how far your ring is from being a PID. It's the group of nonzero (fractional) ideals under multiplication modulo the subgroup of principal ideals. It's known that the class group is finite, and its order is called the class number. The class number is 1 if and only if this ring is a PID. Determining number rings, like the $\mathbb{Z}[\sqrt{d}]$ we have seen, with class number 1 is a problem due to Gauss! Of course, he used different language.

A beautiful result of Heegner, with errors corrected by Stark, completely classifies the imaginary quadratics (i.e. $d<0$) with class number 1. One subtlety, which is a bit hard to explain the precise purpose of, is that when $d \equiv 1 \pmod 4$ we'd rather work with $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ than $\mathbb{Z}[\sqrt{d}]$. Essentially, $\frac{1+\sqrt{d}}{2}$ satisfies the monic integer equation $x^2-2x+\frac{1-d}{4}$ when $d \equiv 1 \pmod 4$.

Let me introduce some notation right now. For $K=\mathbb{Q}(\sqrt{d})$ with d squarefree we will denote its *ring of integers*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}] & \text{otherwise} \end{cases}$$

The set of $d<0$ squarefree so that the associated quadratic ring $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a PID is

$$d \in \{-1,-2,-3,-7,-11,-19,-43,-67,-163\}$$

First, it's incredible that this is even finite! Furthermore, the proof involves an incredible connection between complex multiplication of elliptic curves, class field theory, and modular functions (namely, the j invariant). As a teaser, the fact that $\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ is a PID is very related to the fact that

$$e^{\pi\sqrt{163}} = 262537412640768743.9999999925007...$$

is super close to an integer!

As a shameless advertisement, I wrote a report for my complex analysis class last year about complex multiplication of elliptic curves and class field theory, which only scratched the surface of this area of math. I didn't mention the class number 1 problem specifically, but some of the key ideas are in there. You can find it on my website here. I'll mention that I made a slight notational error in these notes - namely that normally an isogeny is defined to be nonzero, but in my report I took it to be any holomorphic group homomorphism between elliptic curves.

On the other hand, the *real* class number 1 problem, i.e. finding which $d>0$ squarefree with $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a PID is very open. It's not even known if there are finitely many. It is suspected that around 76% of primes which are 1 mod 4 have that $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$ is a PID.

(5) Not many mistakes, so I'll again just make some remarks. Notably, a step I saw many people take was to take a prime $p \equiv 3 \pmod 4$ that divides a sum of squares a^2+b^2 and try to

determine the power of p that appears in the factorization. This is done by factoring $a^2+b^2 = (a+bi)(a-bi)$. Suppose that $p^e||a^2+b^2$. Recall that this means e is the highest power of p dividing a^2+b^2. Now, we critically use the fact that $p \equiv 3 \pmod 4$ implies that p is a prime element of $\mathbb{Z}[i]$.

Suppose $p^f||a+bi$ and $p^g||a-bi$, which we can make sense of by unique factorization of $\mathbb{Z}[i]$ and primality of p in this ring. Then $f+g=e$. Furthermore, there is an automorphism $\mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]$ sending $i \mapsto -i$. Indeed, this is the restriction of complex conjugation $\mathbb{C} \longrightarrow \mathbb{C}$. This map takes $p \mapsto p$ and $a+bi \mapsto a-bi$. Again using that $\mathbb{Z}[i]$ is a UFD, we have that the factorization of $a+bi$ is the complex conjugate of the factorization of $a-bi$. Hence, $f=g$ so $e=2f$ is even.

The reason I wanted to mention this proof is that it uses a critical idea in algebraic number theory. Namely, exploit symmetries of the ring you are factoring in to conclude facts about factorization! Here we used the symmetry of complex conjugation. Formally, we will need Galois theory to explain this, but if you're curious you can look up "Hilbert's ramification theory" or "splitting of prime ideals in Galois extensions".

(6) There weren't many errors here, so I'll remark that though 6 does not have a unique prime factorization, we can factor the ideal (6) in $\mathbb{Z}[\sqrt{-5}]$ as

$$(6) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 2+\sqrt{-5})$$

This is a factorization into prime ideals, and in fact it is unique. Explaining precisely how works is too technical, but you can verify that it is true. You can look up the "Kummer-Dedekind theorem" for information about how this works.

(7) Not many mistakes, so I'll ramble again. For part (b), my preferred proof is to compute the quotient by $\mathfrak{P}$. I do this via the isomorphism $\mathbb{Z}[x]/(x^2+5) \longrightarrow \mathbb{Z}[\sqrt{-5}]$ via $\overline{x} \mapsto \sqrt{-5}$. Then

$$\mathbb{Z}[\sqrt{-5}]/\mathfrak{P} \cong \frac{\mathbb{Z}[x]/(x^2+5)}{(2, \overline{x}+1)}$$

We rewrite the denominator as

$$(2, \overline{x}+1) = (2, x+1, x^2+5)/(x^2+5)$$

so that we may apply the third isomorphism theorem

$$\begin{aligned} \frac{\mathbb{Z}[x]/(x^2+5)}{(2, x+1, x^2+5)/(x^2+5)} &\cong \mathbb{Z}[x]/(2, x+1, x^2+5) \\ &\cong \mathbb{Z}/2\mathbb{Z}[x]/(x+1, x^2+5) \\ &\cong \mathbb{Z}/2\mathbb{Z} \end{aligned}$$

which is a field.

For part (c), my preferred proof for $\mathfrak{P}$ not being principal uses norms. Indeed, suppose $\mathfrak{P} = (\alpha)$. We have that $(2) = \mathfrak{P}^2$ so $(\alpha^2) = (2)$. Furthermore, $N(2) = 4$. Thus, $N(\alpha) = 2$. However, if $\alpha = a + b\sqrt{-5}$ then $N(\alpha) = a^2 + 5b^2$, which can never achieve the value 2 for $a, b \in \mathbb{Z}$.

(8) This was a challenging problem, and the main error was just not rigorously proving the hypothesized characterization, so I'll present a (mostly) detailed proof.

First off, recall that $\mathbb{Z}[i]$ is a PID, so I'll freely use unique factorization, primality, etc.

Let's start with the following question: which primes $p \in \mathbb{Z}$ are also primes in $\mathbb{Z}[i]$? This is equivalent to (p) being a maximal ideal, i.e. to $\mathbb{Z}[i[/(p)$ being a field. Critically, there is an isomorphism $\mathbb{Z}[x]/(x^2+1) \longrightarrow \mathbb{Z}[i]$ which sends $\overline{x} \mapsto i$. Thus, $\mathbb{Z}[i]/(p) \cong \frac{\mathbb{Z}[x]/(x^2+1)}{(p)}$. On the right hand side, (p) is the ideal generated by p in $\mathbb{Z}[x]/(x^2+1)$. To write this in terms of the correspondence principle, we have $p\frac{\mathbb{Z}[x]}{(x^2+1)} = (p, x^2+1)/(x^2+1)$. Hence, by the third isomorphism theorem,

$$\frac{\mathbb{Z}[x]/(x^2+1)}{(p)} \cong \frac{\mathbb{Z}[x]}{(p, x^2+1)}$$

Applying this same procedure will yield an isomorphism

$$\frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2+1)} \cong \frac{\mathbb{Z}[x]}{(p, x^2+1)}$$

Hence, we deduce

$$\mathbb{Z}[i]/(p) \cong \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2+1)}$$

Here's a more rigorous (and general) proof of this sort of thing:

Theorem 0.1. *Let R be a commutative ring and let $f, g \in R$. Then we have isomorphisms*

$$\frac{R/(f)}{(g+(f))} \cong \frac{R/(g)}{(f+(g))} \cong \frac{R}{(f,g)}$$

That is, to compute $R/(f,g)$ we can first mod out by f and then g, or by g and then f. It may be more evocative (though perhaps less clear) to write this first isomorphism as

$$\frac{R/(f)}{(\overline{g})} \cong \frac{R/(g)}{(\overline{f})}$$

And if we're allowing abuse of notation (like conflating elements of quotients with their representatives), we could write

$$\frac{R/(f)}{(g)} \cong \frac{R/(g)}{(f)}$$

Proof. We define maps

$$R \longrightarrow R/(f) \longrightarrow \frac{R/(f)}{(g+(f))}$$
$$R \longrightarrow R/(g) \longrightarrow \frac{R/(g)}{(f+(g))}$$

via the canonical epimorphisms. That is, they take

$$r \mapsto r+(f) \mapsto (r+(f))+(g+(f))$$
$$r \mapsto r+(g) \mapsto (r+(g))+(f+(g))$$

This is truly horrendous notation, but it's the price we pay for rigor. Here, the sum $(r+(f))+(g+(f))$ is not the sum in $R/(f)$, but the coset represented by $r+(f)$ in the quotient $\frac{R/(f)}{(g+(f))}$. We could also write this as

$$r \mapsto \overline{r} \mapsto \overline{\overline{r}}$$

In any case, I hope it's clear that I'm just composing two quotient maps (what Elman calls "canonical epimorphisms").

Both these maps are compositions of two surjections and are hence surjections themselves. We claim that both have kernel (f,g). Let's focus on the first composition

$$R \longrightarrow R/(f) \longrightarrow \frac{R/(f)}{(g+(f))}$$

We want to compute the preimage of $\{0\}$ in $\frac{R/(f)}{(g+(f))}$. Under the map $R/(f) \longrightarrow \frac{R/(f)}{(g+(f))}$, the preimage of $\{0\}$ is the kernel $(g+(f))$. The question then is given $\pi : R \longrightarrow R/(f)$, what is $\pi^{-1}[(g+(f))]$? To deduce this, we introduce the following useful lemma.

Lemma 0.2. *Let $\pi : R \longrightarrow S$ be a surjective map of rings. Let $I \subseteq R$ be an ideal. Then*

$$\pi^{-1}[\pi[I]] = I + \ker(\pi)$$

Proof. Surely $I + \ker(\pi) \subseteq \pi^{-1}[\pi[I]]$. On the other hand, let $r \in \pi^{-1}[\pi[I]]$. Then $\pi(r) \in \pi[I]$. Hence, there is an $a \in I$ so that $\pi(r) = \pi(a)$, so that $r - a \in \ker(\pi)$. We have shown that $r \in I + \ker(\pi)$, so $\pi^{-1}[\pi[I]] \subseteq I + \ker(\pi)$. □

Now, take $\pi : R \longrightarrow R/(f)$ as above. Then the ideal $(g+(f))$ is the image of (g), i.e. $(g+(f)) = \pi[(g)]$. Thus, by the formula in the lemma, we have

$$\pi^{-1}[(g+(f))] = (g) + \ker(\pi)$$

and $\ker(\pi) = (f)$, so this is (f,g). In conclusion, the kernel of

$$R \longrightarrow R/(f) \longrightarrow \frac{R/(f)}{(g+(f))}$$

is (f,g). Thus, by the first isomorphism theorem, there is an isomorphism

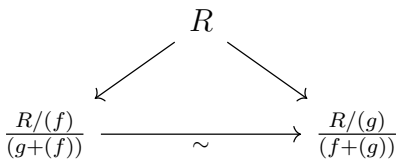
$$R/(f,g) \xrightarrow{\sim} \frac{R/(f)}{(g+(f))}$$

Explicitly, this takes $r+(f,g) \mapsto (r+(f))+(g+(f))$.

A symmetric argument (swapping f and g) will show that $R/(f,g) \cong \frac{R/(g)}{(f+(g))}$ via $r+(f,g) \mapsto (r+(g))+(f+(g))$. Thus, we have isomorphisms

$$\frac{R/(g)}{(f+(g))} \xleftarrow{\sim} \frac{R}{(f,g)} \xrightarrow{\sim} \frac{R/(f)}{(g+(f))}$$

So we deduce our desired isomorphism, and have in fact shown that it is of the form $(r+(g))+(f+(g)) \mapsto (r+(f))+(g+(f))$. We also showed a bit more, that these two are isomorphic not just as rings but as "R-algebras", i.e. we have



□

Remark. All these isomorphisms can be shown more easily and meaningfully, in my eyes, by the "Yoneda lemma" in category theory by computing the functors $\mathsf{CRing}(S, -)$ for the various rings S above. They will all be in bijection to maps out of R which vanish on f and g.

This is a critical isomorphism. The factorization of p in $\mathbb{Z}[i]$ will yield ring theoretic facts about the quotient $\mathbb{Z}[i]/(p)$, say by the Chinese remainder theorem. Similarly, the factorization of x^2+1 in $\mathbb{Z}/p\mathbb{Z}[x]$ will yield ring theoretic facts about the quotient $\frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2+1)}$. The key then is to parlay these factorization facts via the isomorphism $\mathbb{Z}[i]/(p) \cong \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2+1)}$.

Here's a down to earth application, resolving our original question.

$$\begin{aligned} p \text{ is prime in } \mathbb{Z}[i] &\iff \mathbb{Z}[i]/(p) \text{ is a field} \\ &\iff \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2+1)} \text{ is a field} \\ &\iff x^2+1 \text{ is irreducible in } \mathbb{Z}/p\mathbb{Z}[x] \end{aligned}$$

In the last equivalence, I used that $\mathbb{Z}/p\mathbb{Z}$ is a field to deduce that $\mathbb{Z}/p\mathbb{Z}[x]$ is a PID.

This is already beautiful and meaningful, but we can go even farther. Indeed, x^2+1 is quadratic and $\mathbb{Z}/p\mathbb{Z}$ is a field, so it's reducible iff it factors into linear terms. oThat's equivalent to it having a root in $\mathbb{Z}/p\mathbb{Z}$. That is, x^2+1 is reducible in $\mathbb{Z}/p\mathbb{Z}[x]$ iff it has a root in $\mathbb{Z}/p\mathbb{Z}$.

So, what is a root of x^2+1 in $\mathbb{Z}/p\mathbb{Z}$? It's an element $a \in \mathbb{Z}/p\mathbb{Z}$ so that $a^2 = -1$. If $p = 2$, we can take $a = 1 = -1$ and factor $x^2+1 = (x+1)^2$. So now suppose p is odd. Then $-1 \neq 1$ so it has order 2 in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. Thus, finding a so that $a^2 = -1$ is equivalent to finding an element of order 4 in $(\mathbb{Z}/p\mathbb{Z})^*$.

Now we recall that this group is cyclic! Hence, it has an element of order 4 iff it 4 divides its order. Its order in $p-1$, so we have determined that x^2+1 is reducible iff $4|p-1$. In other words, iff $p \equiv 1 \pmod 4$.

Putting this all together, we have determined that p is a prime in $\mathbb{Z}[i]$ iff $p \equiv 3 \pmod 4$.

We can take this a bit farther too to reduce the possibilities of how primes factor in $\mathbb{Z}[i]$. Suppose $p = \prod \pi_i^{e_i}$ is the factorization in $\mathbb{Z}[i]$ for p a prime of $\mathbb{Z}$. Then by the Chinese remainder theorem, we have

$$\mathbb{Z}[i]/(p) \cong \prod \mathbb{Z}[i]/(\pi_i^{e_i})$$

Furthermore, as before, we have that

$$\mathbb{Z}[i]/(p) \cong \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2+1)}$$

The right hand side is a two dimensional vector space over the field $\mathbb{Z}/p\mathbb{Z}$ generated by 1 and $\overline{x}$. Furthermore, each $\mathbb{Z}[i]/(\pi_i^{e_i})$ is a vector space over $\mathbb{Z}/p\mathbb{Z}$. In particular, there can be at most two factors in this product, as we have at most two dimensions over $\mathbb{Z}/p\mathbb{Z}$ to play with. Furthermore, $1, \overline{\pi}_i, \ldots, \overline{\pi}_i^{e_i-1}$ are linearly indepedent over $\mathbb{Z}/p\mathbb{Z}$, so $e_i \leq 2$ is needed as well. We conclude that the only possible factorizations of p in $\mathbb{Z}[i]$ are $p = (\pi^2)$ for π a Gaussian prime with $\mathbb{Z}[i]/(\pi) \cong \mathbb{Z}/p\mathbb{Z}$, $p = \pi_1\pi_2$ for Gaussian primes π_1, π_2 with $\mathbb{Z}[i]/(\pi_i) \cong \mathbb{Z}/p\mathbb{Z}$, or that p remains prime in $\mathbb{Z}[i]$ with $\mathbb{Z}[i]/(p)$ a field extension of $\mathbb{Z}/p\mathbb{Z}$ of dimension 2. Essentially, the factorization possibilities are bounded by 2 because $\mathbb{Q}[i]$ is a 2 dimensional vector space over $\mathbb{Q}$. This generalizes to the "efg" formula, which you can look up.

Anyways, back to the problem itself. Take a (nonzero) prime π in $\mathbb{Z}[i]$. Then (π) is a nonzero prime ideal so $(\pi) \cap \mathbb{Z}$ is also a prime ideal. Observe that $\pi\overline{\pi} \in (\pi)$ and $\pi\overline{\pi} = N(\pi)$ is a nonzero integer. Thus, $(\pi) \cap \mathbb{Z}$ is nonzero and is hence equal to (p) for some integral prime p. That is, every Gaussian prime π is divisible by an integral prime p. We say π "lies over" p.

This lets us stratify the problem. Fix a prime $p \in \mathbb{Z}$. We will classify all the primes "lying over" p, i.e. in its factorization in $\mathbb{Z}[i]$. These are the prime (π) of $\mathbb{Z}[i]$ which contain (p). By the correspondence principle, we are therefore left to understand the prime ideals of the quotient $\mathbb{Z}[i]/(p)$. Recall from above that this is isomorphic $\frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2+1)}$. Since we want to explicitly determine the primes, we should explicitly know this isomorphism. Indeed, elements of $\mathbb{Z}[i]/(p)$ are of the form $a+bi+p\mathbb{Z}[i]$ and elements of $\frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2+1)}$ are of the form $f+(x^2+1)$ for $f \in \mathbb{Z}/p\mathbb{Z}[x]$. We have an isomorphism

$$\begin{aligned} \mathbb{Z}[i]/(p) &\longrightarrow \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2+1)} \\ a + bi + p\mathbb{Z}[i] &\mapsto (a + p\mathbb{Z}) + (b + p\mathbb{Z})x + (x^2 + 1) \end{aligned}$$

Apologies for the messy notation. I'm just saying to take a and b mod p and replace i with the class of x mod $x^2 + 1$.

We proceed as before. If $p = 2$, this polynomial factors as $(x + 1)^2$ so the only prime ideal of $\mathbb{Z}/2\mathbb{Z}[x]/(x^2 + 1)$ is $(x + 1)/(x^2 + 1)$. Under the isomorphism to $\mathbb{Z}[i]/(2)$, we have shown that the only prime ideal of this quotient is $(i+1)/(2)$. As such, the only Gaussian prime lying over 2 is $i + 1$. Indeed, $(i + 1)^2 = (2)$.

If $p \equiv 3 \pmod 4$ then as before, p is itself a Gaussian prime so it is of course the only prime lying over itself.

If $p \equiv 1 \pmod 4$ then as shown above, $\mathbb{Z}[i]/(p) \cong \mathbb{Z}/pZ[x]/(x^2 + 1)$ will be isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Hence, the factorization of p must be of the form $p = \pi_1\pi_2$ with π_i non-associate. Furthermore,

$$\pi_1\pi_2 = p = \overline{p} = \overline{\pi_1\pi_2}$$

Hence, up to associates, $\pi_1 = \overline{\pi_2}$ and vice versa. It follows then (as units have norm 1) that $p = N(\pi_1)$, so p is a sum of squares.

This completes our classification of the Gaussian primes. They are either $1 + i$, an integral prime p which is 3 mod 4, or a Gaussian integer $a + bi$ so that $a^2 + b^2$ is a prime, which is necessarily 1 mod 4.