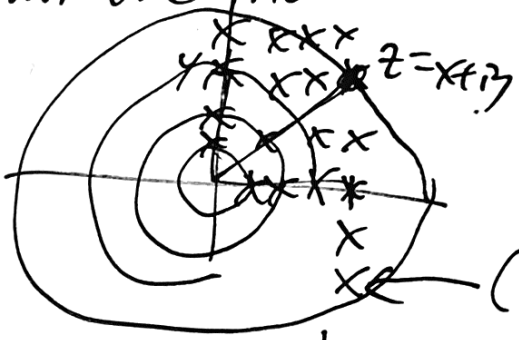
Review: Pyth triples $\rightsquigarrow$ (Rational pts on circle)

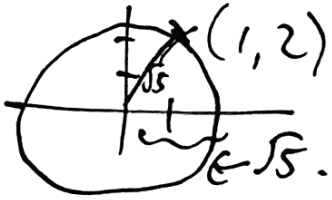
$\rightsquigarrow$ what #s are hypotenuses? $z = r^2 + s^2$. $\rightsquigarrow$

When is $z = x^2 + y^2$? What norms are there of Gaussian integers?

If $z = x+iy \in \mathbb{Z}[i]$, $\Rightarrow N[z] = x^2+y^2 = |z|^2$.



So solving $z = x^2+y^2$ is equivalent to: what radii give circles having lattice points? Already saw: If $n \equiv 3 \pmod 4$, then $n = x^2+y^2$ has no solutions! (So circles centered at $(0,0)$ of radius $\sqrt{n}$ have no grid points.) But, e.g. does circle of radius $\sqrt{5}$ have lattice points? $z = 1+2i$



More foreshadowing: For a general binary quadratic form, $Ax^2+Bxy+Cy^2$. (E.g. $A=1, B=0, C=1$) which n are represented? $n =$

Back to Fundamental Theorem of Arithmetic:

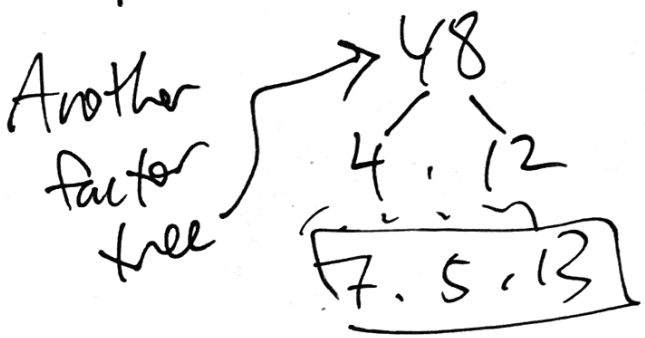
First: Lemma: Every $n \in \mathbb{Z} \setminus \{0\}$ is $\pm 1 \times$ product of primes.

pf: If $n < 0$, replace n by $-n$. I.e. Assume $n > 0$.

If n = prime, done. If not, then $n = m \cdot k$ with both $1 < m$ & $k < \frac{n}{2} < n$. Keep going. Can't continue forever decreasing positive integers.

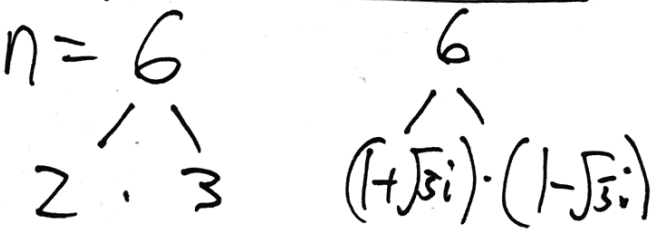
E.g. $n = -48 \rightsquigarrow n = 48$

Another factor tree



How do we know that different factor trees don't at the "bottom" contain different primes?

Non. E.g.: $R = \mathbb{Z}[\sqrt{-5}]$. Take $n = 6$



Fundamental Theorem of Arithmetic: If $n \in \mathbb{Z} \setminus \{0\}$ and $\varepsilon = \varepsilon' \in \{0,1\}$

$$n = (-1)^{\varepsilon} \prod_p p^{e_p} \quad \& \quad n = (-1)^{\varepsilon'} \cdot \prod_p p^{e_p'} \Rightarrow \forall p. \boxed{e_p = e_p' = \mathrm{ord}_p(n)}$$

Recall: $\mathrm{ord}_p(n) = k \iff p^k \| n \iff \left(p^k \mid n \ \& \ p^{k+1} \nmid n\right)$.

Proved: If p = prime, then $\mathrm{ord}_p(a \cdot b) \overset{(*)}{=} \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$.

Pf (FTA): Fix a prime q, take ord_q of 3-sides:

$$\mathrm{ord}_q(n) = \mathrm{ord}_q\left((-1)^{\varepsilon} \prod_p p^{e_p}\right) = \mathrm{ord}_q\left((-1)^{\varepsilon'} \prod_p p^{e_p'}\right). \text{ By } (*),$$

$$\mathrm{ord}_q(n) = \underbrace{\mathrm{ord}_q((-1)^{\varepsilon})}_{0} + \underbrace{\mathrm{ord}_q(2^{e_2}) + \mathrm{ord}_q(3^{e_3}) + \cdots + \mathrm{ord}_q(p^{e_p}) + \cdots}_{0+0+0 \cdots \text{ until } p=q,\ \text{when } \mathrm{ord}_q(q^{e_q}) = e_q.} = \underbrace{\mathrm{ord}_q((-1)^{\varepsilon'})}_{0} + \sum_p \underbrace{\mathrm{ord}_q(p^{e_p'})}_{0+0+0+\mathrm{ord}_q(q^{e_q'})+0+0} = e_q'.$$

$$\mathrm{ord}_q(n) = e_q = e_q'.$$

Q: Where does this proof fail for $R = \mathbb{Z}[\sqrt{5}i]$?

Look at $\text{ord}_2(6)$ Does $2 \mid 6$? Yes, $2 \cdot 3 = 6$.

Does $2^2 \mid 6$? ie. $4(x + \sqrt{5}iy) = 6$? $\Rightarrow 4x = 6$ (from real parts) & $4\sqrt{5}y = 0$ (from imaginary parts) $\Rightarrow y = 0$

no solution.

$2^2 \nmid 6$

So $\text{ord}_2(6) = 1$.

But $6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$

What is $\text{ord}_2(1 + \sqrt{5}i)$? i.e. Does $\exists\, x + \sqrt{5}iy \in \mathbb{Z}[i, \sqrt{5}]$ with.

$2 \cdot (x + \sqrt{5}iy) = 1 + \sqrt{5}i$? Real parts $\Rightarrow 2x = 1$ & $2\sqrt{5}y = \sqrt{5}$.

No solutions in $x, y \in \mathbb{Z}$.

So $\text{ord}_2(1 + \sqrt{5}i) = 0$. **Exercise 1:** Compute $\text{ord}_2(1 - \sqrt{5}i)$.

So $\text{ord}_2(1 + \sqrt{5}i) = 0$ & $\text{ord}_2(1 - \sqrt{5}i) = 0$ But

$\text{ord}_2[(1 + \sqrt{5}i)(1 - \sqrt{5}i)] = \text{ord}_2(6) = 1$ & $0 + 0 \neq 1$.

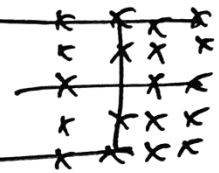
Wait! Is 2 even a prime in $\mathbb{Z}[\sqrt{5}i]$?

What does this even mean?

Try this: $\exists\ (a+\sqrt{5}i\,b)(c+\sqrt{5}i\,d) = 2$? With neither $a+\sqrt{5}i\,b$ nor $c+\sqrt{5}i\,d$ being units.

Recall: $u \in R$ is a unit $\Leftrightarrow \exists\ v \in R$ with $u \cdot v = 1$.

Exercise 2: Compute a set of units of $\mathbb{Z}[i]$



Exercise 3: " " " " " $\mathbb{Z}[\sqrt{5}i]$

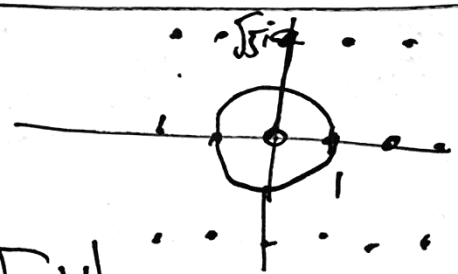
$\frac{1}{\sqrt{5}} \cdot (-i) \cdot \sqrt{5}i = 1$.

$\frac{1}{\sqrt{5}}(-i) \notin \mathbb{Z}[\sqrt{5}i]$.

If $\frac{1}{\sqrt{5}}(-i) \in \mathbb{Z}[\sqrt{5}i]$ then $\exists\ x+\sqrt{5}iy = \frac{-1}{\sqrt{5}}i$.

$\Rightarrow x=0$ & $y\sqrt{5} = \frac{-1}{\sqrt{5}} \Rightarrow y = \frac{-1}{5} \notin \mathbb{Z}$

What does $\mathbb{Z}[\sqrt{5}i] \subset \mathbb{C}$?



Exercise 4: If $z = (a+\sqrt{5}i\,b)(c+\sqrt{5}i\,d)$ with $a,b,c,d \in \mathbb{Z}$, then one of ~ or ~ is a unit (i.e. $= \pm 1$).