The ring $\mathbb{Z}[x]$

$\mathbb{Z}[x]$ is an example of a ring which is not a Euclidean domain for any Euclidean valuation, but is is a UFD.
More generally $R[x]$ is a UFD whenever R is a UFD.
To see that degree is not a Euclidean valuation, we cannot write

$$x^2 = q(x)(2x+1) + r(x) \quad \text{with } r(x) \in \mathbb{Z} \text{ and}$$

$$q(x) \in \mathbb{Z}[x].$$

Because $\mathbb{Z}[x]$ is a UFD, any polynomial in $\mathbb{Z}[x]$ can be written essentially uniquely as a product of irreducibles in $\mathbb{Z}[x]$. The only units in $\mathbb{Z}[x]$ are ± 1

Particularly interesting cases are the polynomials

$x^n - 1 \qquad n \in \mathbb{Z}_+$

$$\text{e.g.} \quad x^2 - 1 = (x-1)(x+1)$$
$$x^3 - 1 = (x-1)(x^2+x+1)$$
$$x^4 - 1 = (x-1)(x+1)(x^2+1)$$

$x^d - 1 \mid x^n - 1$ in $\mathbb{Z}[x] \iff d \mid n$. If $n = dk$ then

$$x^n - 1 = (x^d - 1)\left(\sum_{i=0}^{k-1} x^{id}\right)$$

~~The~~ To write $x^n - 1$ as a product of irreducibles we use the *cyclotomic* polynomials $\Phi_d(x)$ for d dividing n. We can define

$$\Phi_d(x) = \gcd_{\mathbb{Z}[x]}\left(\cancel{x^d-1},\ \sum_{k=0}^{d/d_1 - 1} x^{kd_1} : 1 \le d_1 < d,\ d_1 \mid d\right)$$

or alternatively

$$\cancel{\Psi_d(x) = \mathrm{lcm}\left(\frac{x^d-1}{x^{d_1}-1} : 1 \le d_1 < d,\ d_1 \mid d\right)}$$

$$\Psi_d(x) = \frac{x^d - 1}{\mathrm{lcm}(x^{d_1}-1 : 1 \le d_1 < d,\ d_1 \mid d)}$$

~~This is also Ψ?~~

We also have $\Psi_d(x) = \prod_{\substack{1 \le r < d \\ \gcd(r,d)=1}} (x - e^{2\pi i r/d})$

or $\Psi_d(x)$ can be defined inductively by

$$x^d - 1 = \prod_{\substack{d_1 \mid d \\ 1 \le d_1 \le d}} \Psi_{d_1}(x)$$

The first 2 definitions make it clear that $\Psi_d(x)$ has integer coefficients, that is, that $\Psi_d(x) \in \mathbb{Z}[x]$ — once we know that $\mathbb{Z}[x]$ is a UFD. The first 2 definitions are clearly equivalent, since if $d = kd_1$ then

$$x^d - 1 = (x^{d_1} - 1) \sum_{i=0}^{k-1} x^{id_1}.$$

The last two properties then follow by induction.

The polynomials $\Psi_d(x)$ might not be irreducible in $\mathbb{Z}_p[x]$ for different primes p e.g.

$$\Psi_2(x) = x^2 + x + 1 = (x-1)^2 \text{ in } \mathbb{Z}_3[x]$$

$$\Psi_4(x) = x^2 + 1 = (x-2)(x-3) \text{ in } \mathbb{Z}_5(x)$$

Integers which are sums of two integer squares

Back to this problem!

Theorem $n \in \mathbb{Z}_+$ is a sum of two integers squares $\Leftrightarrow n = N^2 2^k \prod_{i=1}^{r} p_i$ where $N \in \mathbb{Z}_+$, $k \in \mathbb{N}$, ~~and if~~ $r \in \mathbb{N}$, and if $r \geq 1$ then p_i is an odd prime with $p_i \equiv 1 \bmod 4$ $\forall\, 1 \leq i \leq r$

In any UFD, prime $\equiv$ irreducible. Recall $\mathbb{Z}[i]$ is a UFD.

We need a characterisation of primes in $\mathbb{Z}[i]$.

Lemma Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then $a+bi$ is prime in $\mathbb{Z}[i]$ $\Leftrightarrow a^2+b^2$ is prime in $\mathbb{Z}$.

Proof. $a+bi$ not prime $\Rightarrow$ $a+bi$ not irreducible

$\Leftrightarrow$ $a+bi = (a_1+b_1 i)(a_2+b_2 i)$ with $a_1^2+b_1^2 \neq 1$ and $a_2^2+b_2^2 \neq 1$ (because $a_1^2+b_1^2 = 1 \Leftrightarrow a_1+b_1 i = \pm 1, \pm i$, the units)

$\Rightarrow a^2+b^2 = (a_1^2+b_1^2)(a_2^2+b_2^2)$ is not prime in $\mathbb{Z}$.

Now suppose $a+bi$ is prime in $\mathbb{Z}[i]$.

$a^2+b^2 = (a+bi)(a-bi)$

If a^2+b^2 is not prime in $\mathbb{Z}$ then $a^2+b^2 = n_1 n_2$ for $n_1, n_2 \in \mathbb{Z}_+$, $n_1, n_2 \geq 2$

$a+bi$ prime $\Rightarrow$ $a-bi$ is prime because $a+bi = \bar{c}_1 \bar{c}_2$ $\Leftrightarrow a-bi = c_1 c_2$ and c_j is a unit $\Leftrightarrow c_j \bar{c}_j = 1 \Leftrightarrow \bar{c}_j$ is a unit.

So $a^2+b^2 = (a+bi)(a-bi)$ must be the prime factorisation of a^2+b^2. Unique factorisation $\Rightarrow n_1 = u(a+bi)$ for a unit u (renumbering n_1 and n_2 if necessary. But the only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$ and $a \neq 0, b \neq 0$. So this is impossible

$\square$

<u>Proof of Theorem</u> It suffices to prove that a square-free integer n is a sum of 2 integer squares $\Leftrightarrow$ the same is true of all the prime integer factors of n.

For if n is prime we have $nm = 1 + k^2$ for some $m, k \in \mathbb{Z}_+$ (page 74)

$\Leftarrow$ already proved (page 74)

$\Rightarrow$ Suppose n is square free, without loss of generality,

and $n = a^2 + b^2 = (a+bi)(a-bi)$

$$a + bi = \prod_{j=1}^{k} a_j + ib_j \quad \text{where } a_j + b_j i \text{ is prime in } \mathbb{Z}[i].$$

Then $a_j^2 + b_j^2$ is prime in $\mathbb{Z}$ and $n = a^2 + b^2 = \prod_{j=1}^{k} (a_j^2 + b_j^2)$

This is the prime factorisation of n $\square$

(87)

Pythagorean Triples

Defn $(a,b,c) \in \mathbb{Z}_+^3$ is a Pythagorean triple if

$$c^2 = a^2 + b^2$$

Examples
$(3,4,5)$ $25 = 9+16$
$(5,12,13)$ $169 = 144+25$
$(7,24,25)$ $625 = 49+576$

If c is even then both a and b are even - because if a and b are odd then $a^2+b^2 \equiv 2 \bmod 4$ and $c^2 \equiv 0 \bmod 4$

So if $2^k | c$ then $2^k | a$ and $2^k | b$

If c is odd then w.l.g. a is odd and b is even.

General example Let $p, q \in \mathbb{Z}_+$ with $q < p$
then $(p^2-q^2, 2pq, p^2+q^2)$ is a Pythagorean triple because

$$(p^2-q^2)^2 + (2pq)^2 = p^4 - 2p^2q^2 + q^4 + 4p^2q^2$$
$$= (p^2+q^2)^2$$

p^2-q^2 and p^2+q^2 ~~If a and c~~ are odd $\Leftrightarrow$ ~~exactly~~ one of p and q is odd.

Theorem (a,b,c) is a Pythagorean triple with a, c odd with (a,b,c) coprime $\Leftrightarrow$ $\exists$ $p, q \in \mathbb{Z}_+$ with $q<p$ and $a = p^2-q^2$, $b = 2pq$, $c = p^2+q^2$ and coprime and p and q have opposite parities (one odd, one even.)

For the examples above we get $(3,4,5) = (a,b,c)$ from $(p,q) = (2,1)$
$(a,b,c) = (5,12,13)$ if $p,q = (3,2)$
$(a,b,c) = (7,24,25)$ if $(p,q) = (4,3)$

Proof of Theorem $\overset{2}{\Leftarrow}$ ~~Assume w.l.g. that a, b, c are coprime~~ -

because ~~$c^2 = a^2+b^2 = a$~~

Suppose that (a,b,c) is a Pythagorean triple with a and c odd and a and b coprime
$c^2 = a^2+b^2 = (a+ib)(a-ib)$
~~If a and~~ ~~Assume first that~~ ~~a and~~ b are coprime
Let ~~$a+ib$~~

Then $c^2 = \prod p_k^2$ where p_k is prime in $\mathbb{Z}[i]$ $\quad (c = \prod p_k)$

If $p_k \mid a+ib$ and $\bar{p}_k \mid a-ib$ then $\bar{p}_k \mid a+ib$

p_k and $\bar{p}_k$ are equivalent only if $p_k = \pm 1 \pm i$

But $p_k \mid c \Rightarrow |p_k|^2 \mid c^2$ and $|\pm1\pm i|^2 = 2$ So $p_k \neq \pm 1 \pm i$

So if $p_k \mid a+ib$ and $\bar{p}_k \mid a+ib$ we have $|p_k|^2 \mid a+ib$

But $|p_k|^2$ is an integer and p_k a and b are coprime.

So if $p_k \mid a+ib$ we must have $p_k^2 \mid a+ib$ since

$p_k^2 \mid c^2$ So $a+ib = (p+qi)^2$ or $i(p+qi)^2$

for some $p, q \in \mathbb{Z}$.

$a = 2pq$ and $b = p^2-q^2$ or $a = p^2-q^2$ and $b = 2pq$

a odd or b even $\Rightarrow a = p^2-q^2$ and $b = 2pq$

Fermat's Theorem for Cubes

Theorem There is no solution to

$$x^3 + y^3 = z^3$$

where x, y, z are all non-zero integers.

Proof Suppose there is a solution. Then there is a solution with x, y, z all coprime with two of x, y, z odd and the other even. Replacing (y, z) by $(-z, -y)$ or (x, z) by $(-z, -x)$, we can assume z even.

We can also assume $|z|$ is minimal with all these properties.

$$x^3 + y^3 = (x+y)(x^2 - xy + y^2) = z^3$$

$\gcd(x, y) = 1 \Rightarrow \gcd(x+y, x) = \gcd(x+y, y) = 1$

$\Rightarrow \gcd(x+y, xy) = 1$

$\gcd(x+y, x^2 - xy + y^2) = \gcd(x+y, (x+y)^2 - 3xy) = 1$ or 3

Case 1 $\gcd(x+y, x^2 - xy + y^2) = 1$

$$x^2 - xy + y^2 = (x + \omega y)(x + \omega^2 y)$$

where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$ $\qquad \omega^2 = \overline{\omega} = -\frac{1}{2} - \frac{\sqrt{3}}{2} i$

$\omega^3 - 1 = 0 \qquad \omega + \omega^2 + 1 = 0$

Write $\mathbb{Z}[\omega] = \{c_1 + c_2\omega : c_1, c_2 \in \mathbb{Z}\}$

$\mathbb{Z}[\omega]$ is a ring, the ring of Eisenstein integers

It is closed under multiplication, since $\omega^2 = -1 - \omega$

$\mathbb{Z}[\omega] = \mathcal{O}[\sqrt{-3}]$ is a Euclidean domain and hence a UFD

Since $x+y$ and x^2-xy+y^2 are coprime we have $x+y = z_1^3$ and $x^2-xy+y^2 = z_2^3$ for $z_1, z_2 \in \mathbb{Z}$.

$$x^2-xy+y^2 = (x+y\omega)(x+y\omega^2)$$

Let p be a prime in $\mathbb{Z}[\omega]$ with $p \mid x+y\omega$

we claim the maximum power p^n dividing $x+y\omega$ has n divisible by 3. For ~~the maximal po~~ this is true for the maximal power p^n or p dividing x^2-xy+y^2.

p and $\bar{p}$ are inequivalent primes unless

$p = \pm(1-\omega)$ or $\pm(1-\omega^2)$ $\quad (1-\omega^2 = -\omega^2(1-\omega))$

But if $1-\omega \mid x+y\omega$ then $(1-\omega)(1-\omega^2) = 3 \mid x^2-xy+y^2$
$= (x+y)^2 - 3xy$

and we are assuming not.

~~So~~ So If $p \mid x+y\omega$ then $\bar{p} \mid x+y\omega$ or $x+y\omega^2$

But $\bar{p} \nmid x+y\omega$ because otherwise $p\bar{p} \mid x+y\omega$ and $\gcd(x,y) > 1$.

So if $p \mid x+y\omega$, $\bar{p} \nmid x+y\omega$ and $p \nmid x+y\omega^2$

So $p \mid x+y\omega \Rightarrow p^n \mid x+y\omega$ for maximal n with $3 \mid n$

So $x+y\omega = \omega^r(x_1+y_1\omega)^3$ for $r = 0, 1$ or 2

$$= \omega^r(\underbrace{x_1^3+y_1^3}_{\text{odd}} - 3x_1y_1^2 + 3\underbrace{x_1y_1(x_1-y_1)}_{\text{even}}\omega)$$

x, y both odd $\Rightarrow$ $t=2$

$t=0 \Rightarrow y$ even and $t=1 \Rightarrow x$ even

So $x+y\omega = 3x_1y_1(x_1-y_1) + 3x_1y_1^2 - x_1^3 - y_1^3$

$+ \omega(\cancel{x_1^3+y_1^3+3x}$
$3x_1y_1^2 - x_1^3 - y_1^3)$

$x = 3x_1^2y_1 - x_1^3 - y_1^3$

$y = 3x_1y_1^2 - x_1^3 - y_1^3$

$x+y = 3x_1^2y_1 + 3x_1y_1^2 - 2x_1^3 - 2y_1^3$

$= 3x_1y_1(x_1+y_1) - 2(x_1+y_1)(x_1^2 - x_1y_1 + y_1^2)$

$= (x_1+y_1)(5x_1y_1 - 2x_1^2 - 2y_1^2)$

$= (x_1+y_1)(2x_1-y_1)(2y_1-x_1)$ — all 3 factors coprime

$x+y = z_1^3 \Rightarrow x_1+y_1 = C^3 \quad 2x_1-y_1 = A^3 \quad 2y_1-x_1 = B^3$

$A^3+B^3 = C^3 \qquad |C^3| < |z|^3$

$|A^3|^3 < |z|^3, \quad |B|^3 < |z|^3$

So contradicts minimality of z.

Case 2 $\gcd(x+y, x^2-xy+y^2) = 3$

$$3 \mid x+y \quad \text{and } 3 \mid x^2+y^2-xy$$

$$x^2+y^2-xy = (x+y\omega)(x+y\omega^2) = (y+x\omega)(y+x\omega^2)$$

$$3 = (2+\omega)(2+\omega^2) \qquad (= (1-\omega^2)(1-\omega))$$

$2+\omega$ is prime and divides $x+y\omega$ or $y+x\omega = \omega(x+y\omega^2)$

W.l.g. (interchanging x and y if necessary) we can

assume $2+\omega \mid x+y\omega$ in $\mathbb{Z}[\omega]$

then $x+y\omega = (2+\omega)(x_1+y_1\omega)$ for $x_1, y_1 \in \mathbb{Z}$

$$x+y\omega = (2x_1-y_1) + \omega(x_1+y_1)$$

x, y odd $\Rightarrow x_1$ even, y_1 odd

So $x+y = 3x_1$. $\quad 3 \mid z$ and z even $\Rightarrow 6 \mid z \Rightarrow \underset{6^3}{\overset{\shortparallel}{216}} \mid z^3$

$$x^2+y^2-xy = (x+y\omega)(x+y\omega^2) = (2+\omega)(x_1+y_1\omega)(2+\omega^2)(x_1+y_1\omega^2)$$

$$= 3(x_1^2 \cancel{+} x_1y_1 + y_1^2) = 3(y_1+x_1\omega)(y_1+x_1\omega^2)$$

$$3x_1 \times 3(x_1^2 \cancel{+} x_1y_1 + y_1^2) = 216 z_1^3 \qquad z = 6z_1$$

$$x_1(\cancel{y}\, x_1^2 - x_1y_1 + y_1^2) = 24 z_1^3$$

We have $3 \nmid x$ and $3 \nmid y$ so $\cancel{9} \nmid 3xy$

and $9 \nmid (x+y)^2 - 3xy$. So $3 \nmid x_1^2 - x_1y_1 + y_1^2$

So $3 \mid x_1$ and x_1 even $\Rightarrow 24 \mid x_1$ because y_1 odd

So $x_1 = 24t_1$

$\cancel{24}t_1 (y_1+24t_1\omega)(y_1+24t_1\omega^2) = \cancel{24} z_1^3$

$\cancel{t_1} \; z$

$t_1 = v_1^3 \quad (y_1+24t_1\omega)(y_1+24t_1\omega^2) = w_1^3$

$\gcd(y_1, t_1) = 1 \Rightarrow \cancel{y_1+24t_1\omega}$ $y_1+24t_1\omega$ $= (x_2+y_2\omega)^3\omega^r$

for $r = 0, 1, \text{ or } 2$ as before.

$y_1+24t_1\omega = \omega^r(x_2^3+y_2^3 - 3x_2y_2^3 + 3x_2y_2(x_2-y_2)\omega)$

This time $r=0$ because y_1 odd and $24t_1$ even

So $8t_1 = x_2y_2(x_2-y_2)$

$8t_1 = (2v_1)^3$

$\Rightarrow$ and x_2, y_2, x_2-y_2 coprime

$\Rightarrow x_2 = C^3 \quad y_2 = A^3 \quad x_2-y_2 = B^3$

$|A|, |B|, |C| < |z|$ contradicts minimality again