

1. Let α and β be rational numbers, with $|\alpha| \leq 1/2$, and let $m > 0$ be an integer such that $\alpha^2 - m\beta^2 = -1 - \delta$ where $0 \leq \delta < 1$. Set $\epsilon := 1$ if $\alpha \geq 0$ and -1 if $\alpha < 0$. Show that if m is not of the form $5n^2$ ($n \in \mathbb{Z}$) then $|(\alpha + \epsilon)^2 - m\beta^2| < 1$.

Deduce that $\mathbb{Z}[\omega]$ is norm-Euclidean when $\omega = \sqrt{6}$, when $\omega = \sqrt{7}$, or when $\omega^2 - \omega + q = 0$ with $q = -4, -5$ or -7 .

For the next three problems, some of the material in D&F, §§9.1–9.5 will be useful. These sections are mostly review of material from MA 503, and it will be assumed from now on—including exams—that you know what's in them.

2. Let R be a UFD, with fraction field K . Suppose you already have computer algorithms for factoring into primes in R and in the polynomial ring $K[X]$. Describe briefly how you would instruct a computer to factor into primes in $R[X]$.

3. Let k be a field, x, y , and z indeterminates.

(a) Let $f(x)$ and $g(x)$ be relatively prime polynomials in $k[x]$. Show that in the polynomial ring $k(y)[x]$, $f(x) - yg(x)$ is irreducible.

(b) Prove that in $k(y, z)[x]$, the polynomial

$$x^4 - yzx^3 + (y^2z^2 - y)x^2 + (y^2z - y)x + y^2z$$

is irreducible. (Hint. Eisenstein, after rearranging.)

4. Let R be an integral domain with fraction field K , let $R[X]$ be a polynomial ring, and let a and b be nonzero elements in R . Prove:

(a) If R is a UFD and $P \subset R[X]$ is a prime ideal with $P \cap R = (0)$, then P is a principal ideal.

(b) $aR \cap bR = abR$ iff the ring $R[X]/(aX - b)$ is an integral domain.

(c) If $c = aq = bp$ is a nonzero common multiple of a and b then c is an l.c.m. of a and b iff $pX - q$ is a prime element in $R[X]$.

(d) An l.c.m. $[a, b]$ exists iff the kernel of the R -homomorphism $\phi: R[X] \rightarrow R[\frac{b}{a}] \subset K$ taking X to $\frac{b}{a}$ is a principal ideal.

5. (a) Prove that if $x \neq 0$ and y are elements in a UFD such that x^2 divides y^2 , then x divides y .

(b) Let k be a field. In the quotient ring $R = k[X, Y, Z]/(Y^2 - X^2Z)$ let $x = \overline{X}$ and $y = \overline{Y}$ be the natural images of X and Y . Show that x^2 divides y^2 in R , but x does not divide y .

(c) Is R an integral domain? (Why?)

6. (Fermat). Find all solutions in positive integers of the equation $y^3 = x^2 + 4$.

Hint. Prove and use the following facts about Gaussian integers.

(i) $a + bi$ is divisible by $1 + i \iff a - b$ is even.

(ii) If $y^3 = x^2 + 4$ ($x, y \in \mathbf{Z}$), then

$$(x + 2i, x - 2i) = \begin{cases} 1 & \text{if } x \text{ is odd} \\ (1 + i)^3 & \text{if } x \text{ is even.} \end{cases}$$

(iii) If $y^3 = x^2 + 4$ then $x + 2i = i^n(a + bi)^3$ for some n, a, b .