Algebraic Number Theory

ants in your pants

Jay Zhao

Contents

1 Algebraic Integers

1.1 Algebraic Numbers and Algebraic Integers

Minimal Polynomial For $\alpha \in \mathbb{C}$ α's minimal polynomial P over $\mathbb{Q}$ is such that:

1. The leading coefficient of P is 1.
2. $P(\alpha) = 0$.
3. $\deg P$ is minimal.

We refer to $\deg P$ as **the degree** of α.

Example:

- $\sqrt{2}$ has the minimal polynomial $x^2 - 2$.
- i has the minimal polynomial $x^2 + 1$.

☐ **Theorem 1.1.1**: $A(\alpha) = 0$ then there exists Q(x) such that $A(x) \equiv Q(x)P(x)$.

Proof: For the sake of contradiction assume otherwise

By polynomial division $A(x) \equiv P(x)Q(x) + R(x)$ where $\deg R(x) < \deg P(x)$ and $R(x) \not\equiv 0$. Then $0 = A(\alpha) = 0Q(\alpha) + R(\alpha) = R(\alpha)$. $R(\alpha) = 0$, this contradicts the minimality of $\deg P(x)$. ∎

☐ **Corollary 1.1.1.1**: P(x) is the minimal polynomial if and only if it is irreducible.

Algebraic Number An algebraic number is any $\alpha \in \mathbb{C}$ which is the root of some polynomial with coefficients in $\mathbb{Q}$. The set of algebraic numbers is denoted $\overline{\mathbb{Q}}$

Algebraic Integer Consider an algebraic number α and its minimal polynomial P. If it turns out the coefficients of P are integers, then we say that α is an algebraic integer.

☐ **Theorem 1.1.2** (Gauss's Lemma): A polynomial is irreducible over the integer if and only if it is irreducible over the rational.

A result of this is that to check that a number is an algebraic integer, it is sufficient to find a monic polynomial with it as a root with integer coefficient.

Rational Integer the elements of $\mathbb{Z}$ are referred to as rational integers.

Example:

$$4, i, \sqrt[3]{2}, \sqrt{2}+\sqrt{3}$$

are all algebraic integers because they are the roots of $x-4$, x^2+1, x^3-2 and $\left(x^2-5\right)^2-24$.

The number $\frac{1}{2}$ has minimal polynomial $x-\frac{1}{2}$, so it's an algebraic number but not ans algebraic integer. It also implies that no monic integer polynomial has $\frac{1}{2}$ as a root.

□ **Lemma 1.1.3** (Rational algebraic integers are rational integers): An algebraic integer is rational if and and only if it is a rational integer. $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$

Proof: For all $n \in \mathbb{Z}$, n is the root of $x-n$. Conversely the minimal polynomial of $\frac{p}{q}$ is $x-\frac{p}{q}$ and so $\frac{p}{q}$ is an algebraic integer only if $\frac{p}{q}$ is an integer. ∎

□ **Lemma 1.1.4**: The algebraic integers $\overline{\mathbb{Z}}$ forms a ring. The algebraic numbers $\overline{\mathbb{Q}}$ forms a field

Proof: ∎

1.2 Number Fields

Number Field A number field K is field containing $\mathbb{Q}$ as a subfield which is a *finite-dimensional* $\mathbb{Q}$ vector space. The **degree** of K is its dimension.

Example: Consider the field $K = Q\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$. This is a field extension of $\mathbb{Q}$, and has degree 2 (the basis being 1 and $\sqrt{2}$).

Note that ($\square$) *over* [$\square$] *means that it is a field of fractions. This difference doesn't matter though because they are the same thing in this context.*

□ **Theorem 1.2.1** (Artin's primitive element theorem): Every number field K is isomorphic to $\mathbb{Q}(\alpha)$ for some algebraic number α.

1.3 Problems

Exercise 1.3.1: Find a polynomial with integer coefficients which has $\sqrt{2}+\sqrt[3]{3}$ as a root

Solution: Let $x=\sqrt{2}+\sqrt[3]{3}$. It must be the case that $\left(x-\sqrt{2}\right)^3=3$. Expanding this we get that $x^3-3\sqrt{2}x^2+6x-2\sqrt{2}=3$. Hence $x^3+6x-3=\sqrt{2}(3x^2+2)$. Squaring both sides:

$$\begin{aligned}\left(x^3+6x-3\right)^2&=2\left(3x^2+2\right)^2\\ \left(x^3+6x-3\right)^2-2\left(3x^2+2\right)^2&=0\\ x^6-6x^4-6x^3+12x^2-36x+1&=0\end{aligned}$$

Exercise 1.3.2 (Brazil 2006): Let p be an irreducible polynomial in $\mathbb{Q}[x]$ and degree larger than 1. Prove that if p has two roots r and s whose product is 1 then the degree of p is even.

Solution: Since $p(r)=0$, $p\left(\frac{1}{r}\right)$ and p is irreducible it must be that p is the minimal polynomial of p and $\frac{1}{p}$.

Let $d=\deg$. Let $a=\frac{[x^0]p}{[x^d]p}$. Consider $ap(x)-x^dp\left(\frac{1}{x}\right)$, the leading coefficient of both $p(x)$ and $x^dp\left(\frac{1}{x}\right)$ is $[x^d]p$ and their degrees are both d. This means that there exists a polynomial with degree less than d for which r is root. Since p is the minimal polynomial of r that polynomial has to be 0.

Hence $ap(x)\equiv x^dp\left(\frac{1}{x}\right)$. First note that 0, 1 and -1 cannot be roots of $p(x)$ as that would mean the polynomial p has a factor of x, $x-1$ or $x+1$.

If $q(x)\mid p(x)$ where $q\in\mathbb{C}[x]$ then $q(x)\mid x^dp\left(\frac{1}{x}\right)$. So $p(x)$ and $p\left(\frac{1}{x}\right)$ must have the same multi-set of roots counting multiplicity.

Consider the classes of roots $a\equiv b$ if $a=b$ or $a=\frac{1}{b}$. The number of times a appears in the multi-set of roots must be the same as number of time $\frac{1}{a}$ appears. So the number of roots that is a part of each class is even. Thus the total number of roots in the multi-set is even.

So the degree of the polynomial is even.

Exercise 1.3.3: Consider n roots of unity $\varepsilon_1, ..., \varepsilon_n$. Assume the average $\frac{1}{n}(\varepsilon_1 + ... + \varepsilon_n)$ is an algebraic integer. Prove that either the average is 0 or $\varepsilon_1 = \cdot = \varepsilon_n$

Solution: Consider when the sum of the roots of unity is not 0 and when not all the roots of unity are the same, we have by the triangle inequality that if the average is $x = \frac{1}{n}(\varepsilon_1 + \varepsilon_2 + ... + \varepsilon_n)$ then $|x| < 1$.

Now consider any conjugate of x, again it it is the sum of roots of unity and $|x'|$ is ≤ 1. Consider the minimal polynomial of x now. The magnitude of the constant term is equal to the magnitude of the product of all the roots. Hence the magnitude of the constant term is less than 1. But it is not 0. So it must not be an integer. So this cannot happen.

The sum of the roots of unity can only be 0 or a root of unity itself, which only happens when all the roots are the same.

Exercise 1.3.4: Which rational numbers q satisfy $\cos(q\pi) \in \mathbb{Q}$

Solution:

$$\cos\left(\frac{2a}{b}\pi\right) = \frac{\varepsilon_b^a + \varepsilon_b^{-a}}{2}$$

$$2\cos\left(\frac{2a}{b}\pi\right) = \varepsilon_b^a + \varepsilon_b^{-a}$$

We have that $\Phi_b(\varepsilon_b^a) = 0$ If there is an integer polynomial P such that $P\left(x + \frac{1}{x}\right) = 0$ where x is ε_b^{-a} then $2\cos\left(2\frac{a}{b}\pi\right)$ must be a algebraic integer.

Luckily the cyclotomic polynomial is symmetric. Which means there does exist such a polynomial.

So $2\cos(q\pi)$ is an integer. But it's also bounded between -1 and 1. This means $\cos(q\pi) = -1, -\frac{1}{2}, \frac{1}{2}, 1$.

Exercise 1.3.5: There are $n > 2$ lamps arranged in a circle; initially one is on and the others are off. We may select any regular polygon whose vertices are among the lamps and toggle the states of all lamps simultaneously. Show it is impossible to turn all lamps off.

We interpret the points of the regular polygon of N sides as the N roots of unity $1 - \omega^0, \omega^1, \omega^2, ...\omega^{N-1}$. Without loss of generality assume that T is the lamp that is turned on at the start. Then let a^i be the number of times lamp i corresponding to the complex number ω^i was toggled. Since for every regular polygon the sum of all the points on the polygon is 0 we should have at the end that $a_0 + a_1\omega_1 + a_2\omega + ... + a_{n-1}\omega^{n-1} = 0$ but also that a_0 is odd while all of $a_1, ..., a_n$ are even. This means that $(2k_0 - 1)a_0 + 2k_1a_1 + ... + 2k_{n-1}a_{n-1} = 0$ This then means that

$$k_0a_0 + k_1a_1 + ... + k_{n-1}a_{n-1} = \frac{1}{2}$$

which is impossible

Exercise 1.3.6: Let α be an algebraic integer. Suppose all its Galois Conjugates have absolute value one. Prove $\alpha^N = 1$ for some positive integer N.

Let P be the minimal polynomial of α, we have that α and all the galois conjugates of α are roots of P. This means that $P(0) = \prod \text{conjugate}(a) = \pm 1$

2 The Ring of Integers

2.1 Galois Conjugates

Galois Conjugates Let α be an algebraic number, and let $P(x)$ be its minimal polynomial of degree m. Then the m roots of P are the galois conjugates of α.

☐ **Lemma 2.1.1**: An irreducible polynomial in $\mathbb{Q}[x]$ has no repeated roots

Norm Let $a \in K$ have degree m, so $\mathbb{Q}(a) \subseteq K$, set $k = \frac{\deg K}{n}$ defined as

$$N_{K/\mathbb{Q}}(\alpha) \coloneqq \left(\prod \text{Galois conj of } \alpha\right)^k$$

Trace

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \coloneqq k \cdot \left(\sum \text{Galois conj of } \alpha\right)$$

These are both "weighted averages" the add up to a weight of k. k is actually an integer because when we adjoin other things to $\mathbb{Q}(a)$ it is a tensor product.

☐ **Lemma 2.1.2**: If α is an algebraic integer, it's norm and trace are rational integers.

Proof: Vieta's Formulas ∎

☐ **Theorem 2.1.3**: Let K be a field of degree n, and let $\alpha \in K$. Let $\mu_\alpha : K \to K$ denote the map $x \mapsto \alpha x$ viewed as a linear map of $\mathbb{Q}$-vector space. Then,

- The **norm** is the determinant $\det \mu_\alpha$
- The **trace** is the trace $\mathrm{Tr}\ \mu_\alpha$

2.2 The Ring of Integers

Ring of Integers Define $\mathcal{O}_K \coloneqq K \cap \overline{\mathbb{Z}}$ that is the set of integers which are algebraic integers and also in the number field K. *This is map of fields to rings of integers*.

Exercise 2.2.1: Let a and b be rational numbers, and d a square free integer.

- If $d \equiv 2, 3 \pmod 4$, prove that $2a, a^2 - db^2 \in \mathbb{Z}$ if and only if $a, b \in Z$.
- For $d \equiv 1 \pmod 4$, prove that $2a, a^2 - db^2 \in \mathbb{Z}$ if and only if $a, b \in \mathbb{Z}$ OR if $a - \frac{1}{2}, b - \frac{1}{2} \in \mathbb{Z}$

If a is an integer it implies db^2 is an integer then $b^2 = \frac{n}{d}$ where d is square free implies that $n = \square \times d$ and hence $b^2 = \square$ and b is an integer. Then obviously if b is an integer so is a.

Now if $d \equiv 2, 3 \pmod 4$ and $2a$ is an integer assume a and b are not integers we have then that $a = \frac{n}{2}$ and $a^2 = \frac{n^2}{4}$. We then have that $\frac{n^2}{4} + m = db^2$ and therefore $n^2 + 4m = 4db^2$ since $\frac{n}{2}$ is not an integer n is not even and hence $n^2 + 4m \equiv 1$ is but $d(2b)^2 \equiv 2, 3, 0 \pmod 4$.

For the case where $d \equiv 1 \pmod 4$ we have that if we assume a is not a integer then again $a = \frac{n}{2}$ where n is odd. $n^2 + 4m = d(2b)^2 \equiv 0, 1 \pmod 4$ the only possible case s when $d(2b)^2 \equiv 1 \pmod 4$ which occurs when $d(2b)^2$ is odd and hence $2b$ is odd and $b = \frac{k}{2}$.

□ **Lemma 2.2.1**: In general the ring of integers of $K = \mathbb{Q}\left(\sqrt{d}\right)$ is

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\sqrt{d}\right] & d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod 4 \end{cases}$$

Example: Consider $K = \mathbb{Q}\left(\sqrt{3}\right)$. We can always rationalize the denominator for any $x \in K$. For instance: $\frac{1}{4+\sqrt{3}} = \frac{4-\sqrt{3}}{13}$.

☐ **Theorem 2.2.2** ($K = \mathbb{Q} \cdot \mathcal{O}_K$): We can rationalize the denominator. Let K be a number field then for any $x \in K$ we have that $x = \frac{1}{n}\alpha$ for some integer n. For some $\alpha \in \mathcal{O}_K$

Proof: ∎

☐ **Lemma 2.2.3** ($a \in \overline{\mathbb{Z}} \iff \mathbb{Z}[\alpha]$): Let $\alpha \in \overline{\mathbb{Q}}$. Then α is a algebraic integer if and only if the abelian group $\mathbb{Z}[\alpha]$ is finitely generated.

This now immediately implies ☐ Lemma 1.1.4

☐ **Theorem 2.2.4**: A number field of degree n. Then $\mathcal{O}_k$ is a $\mathbb{Z}$-module of rank n.

2.3 Problems

Exercise 2.3.1: Show that α is a unit of $\mathcal{O}_K$ (meaning $a^{-1} \in \mathcal{O}_K$) if and only if $N_{K/\mathbb{Q}(\alpha)} = \pm 1$.

Assume otherwise then since $|N(\beta)| \geq 1$ for all $\beta \in \mathcal{O}_K$ which means that $N(\alpha\beta) = N(\alpha)N(\beta) \neq 1$ and hence $\alpha\beta$ cannot be 1.

Then if $N(\alpha) = \pm 1$ then the product of it with its galois conjugates is ± 1. If it's -1 we can scale it by -1, so the product of all the other galois conjugates is the inverse of α.

Exercise 2.3.2: Let K be a number field. What is the field of fractions of $\mathcal{O}_K$

K.

Exercise 2.3.3: Find all integers m and n such that $\left(5 + 3\sqrt{2}\right)^m = \left(3 + 5\sqrt{2}\right)^n$

Taking the norm over the ring of integers $\mathbb{Z}\left[\sqrt{3}\right]$ we have that $7^m = (-41)^n$ which means that $m, n = 0$.

3 Unique Factorization

3.1 Ideal Arithmetics

In this section we work with ideals of $\mathcal{O}_K$, which we will write $\mathfrak{a}, \mathfrak{b}$ and $\mathfrak{p}, \mathfrak{q}$ for prime ideals.

$$\mathfrak{a} + \mathfrak{b} \coloneqq \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$$
$$\mathfrak{a} \cdot \mathfrak{b} \coloneqq \{a_1 b_1 + \ldots a_n b_n \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

That is given $\mathfrak{a} = (a_1, a_2, \ldots, a_n)$ and $\mathfrak{b} = (b_1, b_2, \ldots, b_m)$ we have that

- $\mathfrak{a} + \mathfrak{b} = (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m)$
- $\mathfrak{a} \cdot \mathfrak{b} = \left(a_i b_j \mid 1 \leq i \leq n, 1 \leq j \leq m\right)$

We'll also let $c\mathfrak{a} \coloneqq \{ca \mid a \in \mathfrak{a}\}$. We'll also say that $\mathfrak{a} \mid \mathfrak{b} \iff \mathfrak{a} \supseteq \mathfrak{b}$.

For example (3) | (15). Also note that prime ideals are ideals where $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

Remark: There is some stuff about Dedekind domains but they look hard as hell.

3.2 Unique Factorization works in Dedekind Domains

This means they work in $\mathcal{O}_K$.

□ **Theorem 3.2.1**: Let $\mathfrak{a}$ be a nonzero proper ideal of a Dedekind domain in $\mathcal{A}$. Then $\mathfrak{a}$ can be written as a finite product of non zero prime ideals uniquely up to ordering.

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_n^{e_n}$$

Moreover $\mathfrak{a}$ divides $\mathfrak{b}$ is and only if for every prime ideal of $\mathfrak{a}$ the exponent of $\mathfrak{p}$ is less than the exponent in $\mathfrak{b}$.

Fractional Ideal A fractional ideal J is a set of the form $\frac{1}{x} \times \mathfrak{a}$ where x is an integer and $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$. We call ideals of $\mathcal{O}_K$ integral ideals, notice that integral ideals are fractional ideals when $x = 1$.

We can thing of fractional ideals as ideals divided out by a denominator.

□ **Theorem 3.2.2**: Fractional Ideals form a inverse under multiplication, with

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \in (1)\}$$

Which is the set of all elements of the field of fractions which resolves the denominator.

The group of ideals is denoted J_K.

Every fractional ideal can be uniquely written as the product of integral ideals and the product of the inverses of integral ideals.

Ideal Norm $|\mathcal{O}_K l\mathfrak{a}| =: N(\mathfrak{a})$. The norm of an ideal is the number of equivalent classes mod that ideal.

Ideal norm is finite, multiplicative and $N((a)) = |N(a)|$.

Two ideals I and J are in the same class if $xI = yJ$ for some elements of $\mathcal{O}_K$. We write $\frac{1}{2}\mathbb{Z} \sim 3\mathbb{Z}$ for example.

Ideal classes form a group under multiplication

3.3 Factorization Algorithm

Remark: Prime ideals are maximal hence $R/\mathfrak{p}$ is a field, this is something we know from Olympiad number theory.

Example: Consider the ring $R = \mathbb{Z}\left[\sqrt{-17}\right]$. We have that $R = Z[x]/\left(x^2 + 17\right)$. We also have that $R/(3) = R/\left(\prod \mathfrak{p}_i^{e_i}\right)$.

$R/(3) = \mathbb{F}_3[x]/\left(x^2 - 1\right) = \mathbb{F}_3[x]/((x-1)(x+1))$.

So the factor of (3) are $(x-1, 3), (x+1, 3)$

□ **Theorem 3.3.1** (Dedekind-Kummer Theorem): Assume that $|\mathcal{O}_\mathcal{K}/\mathbb{Z}[\theta]| = j$ where $j < \infty$. and p¬ dividing j.

$$(p) = \prod (f_i(\theta), p)^{e_i} \pmod{p}$$

3.4 Problems

Exercise 3.4.1: Show that there are three different factorizations of 77 in $\mathcal{O}_K$, where $K = \mathbb{Q}\left(\sqrt{-13}\right)$.

So first note that as $-13 \equiv 3 \pmod 4$ hence $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{-13}\right]$. Then we'll use the factoring theorem with $\theta = \sqrt{-13}$. $x^2 + 13 \equiv x^2 - 1 \pmod 7$. $(7) = \left(\sqrt{-13} - 1, 7\right)\left(\sqrt{-13} + 1, 7\right)$. The similarly $x^2 + 13 \equiv x^2 - 9 \pmod{11}$. $(11) = \left(\sqrt{-13} - 3, 11\right)\left(\sqrt{-13} + 3, 11\right)$. $(77) = \left(\sqrt{-13} - 3, 11\right)\left(\sqrt{-13} + 3, 11\right)\left(\sqrt{-13} - 1, 7\right)\left(\sqrt{-13} + 1, 7\right)$.

4 An Orthodox Introduction to Algebraic Number Theory

https://www.youtube.com/watch?v=bDs-74plu5A&list=PLSibAQEfLnTwq2-zCB-t9v2WvnnVKd0wn&index=7

Minkowski's Theorem Every convex set $\mathbb{R}^n$ which is symmetric about the origin and which has volume greater than 2^n contains a non-zero integer point.

This can be extended to any any lattice with volume greater than $2^n d(L)$ where $d(L)$ is the determinant of a basis.

Exercise 4.1: Characterise all solution to $a^2 + b^2 = c^2$ over the integers.

Notice that if $(a, b, c) = (a'g, b'g, c'g)$ is a solution then so is (a,b,c). So consider for now only when $(a, b, c) = 1$. If a and b are both divisible by prime p then $p \mid a^2 + b^2$ and so $p \mid c$ as well. Hence $(a, b) = 1$.

Now taking mod 4 we cannot have both a and b odd as that would imply $c^2 \equiv a^2 + b^2 \equiv 1 + 1 \equiv 2 \bmod 4$ which is a contradiction.

Hence $a + b$ and $a - b$ is odd. Now consider the number field $K = \mathbb{Q}\left(\sqrt{-1}\right)$ or simply $\mathbb{Q}(i)$ with the associated ring of integers $\mathcal{O}_K = \mathbb{Z}[i]$. This is a UFD.

$(a + ib)(a - ib) = c^2$. Notice that if a prime p divides both $(a + ib)$ and $(a - ib)$ then $p \mid 2a$ and $p \mid 2ib$. Notice if $p \mid 2$, the norm of $a + ib$ is $a^2 + b^2$ and the norm of p is a multiple of 2 then $a^2 + b^2$ is a multiple of 2 contradiction. So $p \nmid 2$ and so $p \mid a$ and $p \mid b$ which means that a and b are not coprime as $(a, b) = (1)$, contradiction. So then $(a + ib)$ and $(a - ib)$ are coprime.

This means that $a + ib = x^2$ for some $x \in \mathbb{Z}[i]$ hence $a + ib = u \cdot (m + ni)^2$ where u is a unit and $m, n \in \mathbb{Z}$.

$$a + ib = u\left(m^2 - n^2\right) + u(2mn)i$$

Which yields the solution set $(a, b) = \left(m^2 - n^2, 2mn\right), \left(2mn, m^2 - n^2\right)$. Which we can rescale to recover all solutions.

Exercise 4.2: Prove that there are no solutions to $a^3 + b^3 = c^3$ over $\mathbb{Z}_{>0}$.

Consider the number field $K = \mathbb{Q}(\omega)$ where $\omega = e^{\frac{2\pi i}{3}}$. The associated number field is $\mathbb{Z}[\omega]$ which happens to be a UFD as it is $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$

Assume by similar reasoning that x and y are coprime. We show that it also has no non trivial solutions over $\mathbb{Z}[\omega]$. $(a+b)(a+\omega b)\left(a+\omega^2 b\right) = c^3$.

We'll write $p = (1-\omega)$. $N(p) = (1-\omega)\left(1-\omega^2\right) = 3$. So $x \equiv 0, 1, -1 \mod p$.

Now $(xp \pm 1)^3 = p^3 x(x \pm 1)(x \pm (1+\omega)) \equiv p^3 x(x \pm 1)(x \mp 1)$ so if $a \equiv \pm 1 \bmod p$ then we must have that $a^3 \equiv \pm 1 \bmod p^4$.

Now if a, b, c are all not divisible by p then $a^3 + b^3 = c^3$ yields a contradiction mod p^4. So $p \mid a$. It follows then that $p \mid a$, $p \mid b$ and $p \mid c$.

This lets us perform infinite descent on $v_p(c)$.

Exercise 4.3: Prove that there are no solutions to $y^3 = x^2 + 5$

First notice that if x or y is a multiple of 5 then $v_5(\text{RHS}) = 1$ but $v_5(\text{LHS})$ is at least 3.

Since we can't factorize directly we factorize ideals.

$(y)^3 = \left(x+\sqrt{-5}\right)\left(x-\sqrt{-5}\right)$. We'll now prove that $\left(x+\sqrt{-5}\right) + \left(x-\sqrt{-5}\right) = (1)$. We'll denote these two ideals as $(a), (b)$, since $2\sqrt{-5} = a - b$ we have that any even multiple of $\sqrt{-5}$ can be formed and hence any multiple of 10 can be formed as a linear combination of a and b. $a + b = 2x$ and since x and 5 are coprime by Bézout all integers are in $(a)(b)$. Now considering mod 4. If x is odd then y^3 is even and 4 divides $x^2 + 5$ but $x^2 + 5 \equiv 2 \bmod 4$. Contradiction! x is even.

Then it's pretty trivial to show that $(a)(b) = (1)$. So this means that each of $\left(x+\sqrt{-5}\right)$ and $\left(x-\sqrt{-5}\right)$ are cubes of ideals.

There are two classes of ideals in $\mathbb{Z}\left[\sqrt{-5}\right]$. So $\left(x+\sqrt{-5}\right) = (a)^3 = \left(a^3\right)$ and $\left(x-\sqrt{-5}\right) = (b)^3 = \left(b^3\right)$. $x + \sqrt{-5} = \left(n + m\sqrt{-5}\right)^3 = \left(x^3 - 15xy^2\right) + \left(3x^2y - 5y^3\right)\sqrt{-5}$.

$3x^2y - 5y^3 = 1$ and $x = 3x^3 - 15xy^2$. So we have that $y\left(2x^2 - 5y^2\right) = 1$ and $x = 3x\left(x^2 - 5y^2\right)$. This is a contradiction.

You can also solve this without the use of ANT by using QR Theory.

Exercise 4.4: Consider the ring $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ (Scaled so that $N(x) = |x|^2$). Show that, for all $0 \neq J, \exists\, 0 \neq a \in J$ such that $\frac{N(\alpha)}{N(J)} \leq 2\frac{\sqrt{7}}{\pi}$, hence this ring is a UFD

Suppose that J is a ideal of this ring and imagine all it's elements on the complex plane. Imagine expanding a circle of growing radius r centered at the origin.

When $\pi r^2 \geq 4 \times$ Area('one of the cells') it's guaranteed that some element of J is in this circle. So pick the equality case

So there is guaranteed to be $N(\alpha) \leq r^2$ where $\pi r^2 = 4 \cdot \frac{\sqrt{7}}{2} \cdot N(J)$. So $\frac{N(\alpha)}{N(J)} \leq \frac{r^2}{r^2} \cdot \frac{2\pi}{\sqrt{7}}$. This means that $\frac{N(a)}{N(J)} \leq 1$ and hence all ideals are in the same class as the one small ideal of Norm 1. Which is principle.

Exercise 4.5 (Fermat's Christmas Theorem): For all primes p there exists $a, b \in \mathbb{Z}$
such that $p = a^2 + b^2$.

Remark: Okay this one is cool as hell.

Using Minkowski's Theorem: Let k be a quadratic residue of $-1 \bmod p$.

Consider the lattice $\{x + yi \in \mathbb{Z}[i] \mid x \equiv yk \mod p\}$. This lattice has determinant p in $\mathbb{R}^2$ as it is generated by the basis $v_1 = (p, 0), v_2 = (k, 1)$.

Now take the unit circle of radius $2\sqrt{\frac{p}{\pi}}$. It is guaranteed to contain a nonzero lattice point as it's area is $4p$. So there exits a lattice point where

$$x \equiv yk \bmod p \text{ and } x^2 + y^2 < \left(2\sqrt{\frac{p}{\pi}}\right)^2 < 2p$$

hence $x^2 + y^2 = p$

Exercise 4.6: Prove that for the rings $\mathbb{Z}\left[\sqrt{3}\right]$, for every ideal J there exists α such that $\frac{|N(\alpha)|}{N(J)} \leq \sqrt{3}$ and for the ring $\mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right]$ the bound will be $\frac{|N(\alpha)|}{N(J)} \leq \frac{\sqrt{13}}{2}$