Number theory and arithmetic geometry

Soham Chowdhury

September 2, 2017

Contents

Part I

Basic notions

Chapter 1

Algebraic integers

> Pellentesque condimentum, magna ut suscipit hendrerit, ipsum augue ornare nulla, non luctus diam neque sit amet urna.
>
> Someone

1.1 Appetizer: Fermat's theorem on sums of two squares

Question 1.1.1. *Does the equation*

$$p = a^2 + b^2 \qquad (p \textit{ prime}) \tag{1.1}$$

have nontrivial solutions with integer a *and* b*?*

A bit of history This section is salvaged from a stray LaTeX file found in an old `/home` folder. I wrote this for a friend at Canada/USA Mathcamp, as part of my usual Number Theory Indoctrination Service.

One start is to look at the equation mod 4. Since squares are always either 0 or 1 modulo 4 (work this out for yourself if it's not familiar) p can only be 1 mod 4. [1] Keeping this in mind, we restrict our attention to primes $\equiv 1 \pmod 4$.
We notice that a nontrivial "factorization" of p of the form

$$p = (a + ib)(a - ib) a, b \in \mathbf{Q}$$

gives us an expression of the form we want, if we are willing to expand our notion of what factorization means beyond its usual meaning in $\mathbf{Z}$. In fact, the approach that we follow is to look at how different primes factor or "split" in the ring $\mathbf{Z}[i]$, which is the ring of numbers of the form

$$\mathbf{Z}[i] = \{a + ib : a, b \in \mathbf{Z}\}$$

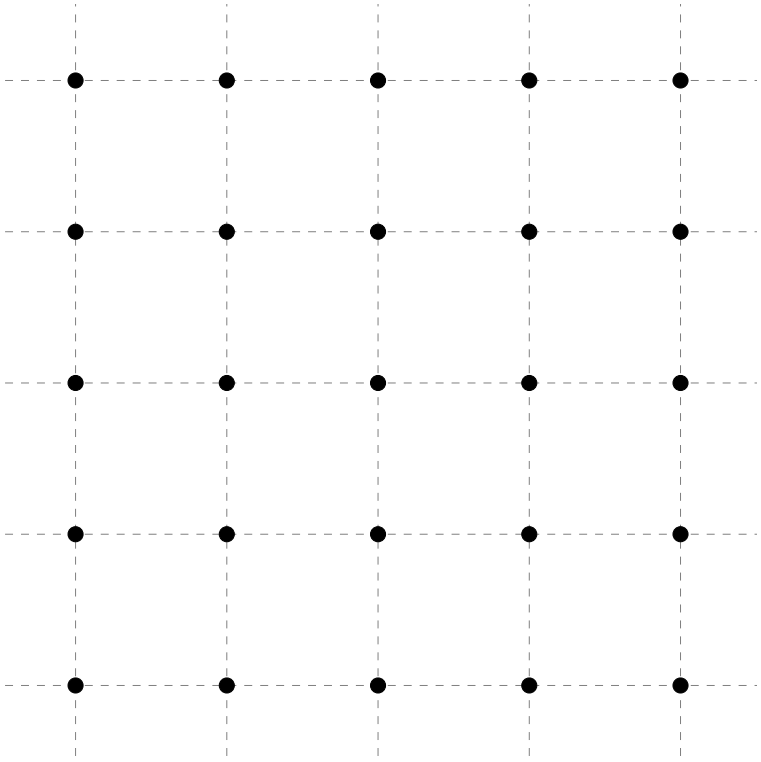
We will obtain a complete description of how integer primes split in this ring, the *ring of Gaussian integers*, and thus prove the following:

Theorem (Fermat)**.** *A prime number can be expressed as a sum of two integer squares iff it is congruent to* 1 *mod* 4*.*

$\mathbf{Z}[i]$ as a lattice

Notice that it can often be worthwhile to think of $\mathbf{Z}[i]$ geometrically, as a subset of the complex plane corresponding to all the complex numbers with integer real and complex parts. This gives $\mathbf{Z}[i]$ the structure of a (square) *lattice*, which has an obvious meaning that we will not work hard to rigorize for now: think of the points in the plane with integer coordinates, where (x, y) corresponds to $x + iy$.

[1] 0 and 2 are, uh, not really possibilities, except in the case $2 = 1^2 + 1^2$.



Aside 1.1.2. This has very deep applications once we start considering more interesting number fields: here we are looking at $\mathbf{Q}(i)$ and its *ring of integers* $\mathbf{Z}[i]$, and $\mathbf{Q}(i)$ is basically the nicest number field in existence. We will see that arguments using the "geometry of numbers", also called *Minkowski theory*, are very powerful, and will (for instance) enable us to prove the Dirichlet unit theorem.

Preliminaries

First, we review a few definitions from ring theory.
For example, 2 is not irred in $\mathbf{Z}[i]$, since $2 = (1+i)^2$, but it is an irred in $\mathbf{Z}$, since the only ways to write it as a product are silly things like $(-1)\cdot(-2)$ and -2 is manifestly a unit times 2.

Definition 1.1.3. A ring R is *Euclidean* if there exists a function

$$\nu : R \setminus \{0\} \to \mathbf{Z}^{\geqslant 0},$$

called the *Euclidean valuation*, such that we can perform a "division algorithm" in the ring using ν.

That is, for any $a, b \in R$, there exist $q, r \in R$ such that[2]

$$a = bq + r, \nu(r) < \nu(b).$$

For instance, $\mathbf{Z}$ is an Euclidean domain with valuation $\nu(r) = |r|$.

Definition 1.1.4. A *principal ideal domain*, or *PID* for short, is a ring where all ideals are generated by a single element (all ideals are *principal*).

Definition 1.1.5. A *unique factorization domain* (often *UFD* for short, or sometimes *factorial* ring or domain) is a ring where elements can be uniquely factored into irreducible elements. That is, for all $r \in R$, there exists a factorization

$$r = u \cdot p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

where u is a unit, and the p_i and a_i are unique, up to reordering of the p_i.

[2]Note that the valuation of 0 is not defined, at least per this definition. However, setting $\nu(0) = 0$ seems to work just fine.

Now, we have:

Theorem 1.1.6. *Euclidean domain $\implies$ PID.*

Proof. Consider an arbitrary ideal I of our ring R. Choose a smallest nonzero element w from I (where "smallest" refers to the valuation being the least).
Any other element of I can be written as

$$a = wq + r$$

where $\nu(r) < \nu(w)$. But there is no such nonzero element, by the assumption that w has the smallest valuation of any element of I. We conclude that $r = 0$. Hence w divides every other element of I, so $I = (w)$. ■

Very Useful Theorem 1.1.7. *PID $\implies$ UFD.*

Proof. The proof is too messy to include here. Some references are provided in the margin. A quick google turned up this pdf. ProofWiki also has an incomplete proof. ■

It's worth taking a moment to do the following (easy) exercise:

Exercise 1.1.A. In any integral domain, primes are irreducible.

There is, in fact, a very important partial converse:

Exercise 1.1.B (and Fact)**.** In a UFD, irreducibles are prime.

This will be helpful shortly. In fact, the only reason why we went to all the trouble with PIDs and so on is so that we could state this fact!

$\mathbf{Z}[i]$ is a UFD

Proposition 1.1.8. *The function $\nu : \mathbf{Z}[i] \to \mathbf{Z}^{\geqslant 0}$ defined by*

$$\nu(a + ib) = a^2 + b^2 = |a + ib|^2$$

is an Euclidean valuation on the ring $\mathbf{Z}[i]$.

Proof. Given $a, b \in \mathbf{Z}[i]$, we need to show that there exist $q, r \in \mathbf{Z}[i]$ such that

$$a = bq + r \qquad\qquad |r|^2 < |b|^2 \tag{1.2}$$

This is equivalent to $\frac{a}{b} - q = \frac{r}{b}$.
We need to find a b such that

$$\left|\frac{a}{b} - q\right| = \left|\frac{r}{b}\right| < 1.$$

Why is this possible? Notice that the number $\frac{a}{b}$ lies in some square of the lattice formed by the Gaussian integers in the complex plane. So there will always be some lattice point within (at most) half the length of a diagonal of a lattice square from $\frac{a}{b}$. This suffices, since that length is $\frac{\sqrt{2}}{2} < 1$. ■

If $p = 4n + 1$ is a prime, then the congruence

$$-1 \equiv x^2 \pmod{p}$$

has a solution: indeed, by Wilson's theorem,

$$\begin{aligned} -1 \equiv (p-1)! &= (1 \cdot 2 \cdots (2n)) \cdot ((2n+1) \cdot (2n+2) \cdots (4n)) && (1.3)\\ &\equiv (1 \cdot 2 \cdots (2n)) \cdot ((-2n) \cdot (-2n+1) \cdots (-1)) && (1.4)\\ &= (2n)! \cdot (-1)^{2n} (2n)! && (1.5)\\ &= [(2n)!]^2 \pmod{p} && (1.6) \end{aligned}$$

so taking $x = (2n)!$ works.
Now we are ready to prove the main theorem. We restate it here:

Theorem 1.1.9 (Fermat)**.** *A prime number can be expressed as a sum of two integer squares iff it is congruent to* 1 *mod* 4*.*

Proof. It now suffices to show that a prime $p \in \mathbf{Z}$ does not remain prime in $\mathbf{Z}[i]$ if $p \equiv 1 \pmod 4$. When that is done, we have a nontrivial factorization

$$p = \alpha \cdot \beta$$

and taking norms (i.e. valuations) of both sides gives

$$p^2 = (a^2 + b^2) \cdot \nu(\beta)$$

where we write $\alpha = a + ib$. Now, since the factorization is nontrivial, neither α nor β are units, and hence we have $p = a^2 + b^2$, and we're done.
But for primes congruent to 1 modulo 4, we have our lemma which states that there exists x such that $x^2 + 1 \equiv 0 \pmod 4$. So $p \mid x^2 + 1 = (x + i)(x - i)$, but it does not divide either of the factors on the right (it doesn't divide either of their imaginary parts). So p is not prime in $\mathbf{Z}[i]$.
Now we use all the algebra we did: since $\mathbf{Z}[i]$ is a UFD, our Fact from before tells us that p not prime implies that p is not irreducible. So p has some factorization

$$p = \alpha \cdot \beta$$

in $\mathbf{Z}[i]$, and we're done. ∎

1.2 Integrality

Let $A \mid B$ be an extension of rings.

Definition 1.2.10. An element $b \in B$ is called integral over A if it satisfies a monic equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

with $a_i \in A$.

Definition 1.2.11. B is integral over A if all $b \in B$ are integral over A.

Definition 1.2.12. The characteristic polynomial of an element α will be denoted χ_α.

Definition 1.2.13. The minimal polynomial of an element α will be denoted μ_α.

The setup

Fix a domain A integrally closed in $K := K(A)$. Let $L \mid K$ be a finite extension, and B the integral closure of A in L. This is the AKLB *diagram*:

$$\begin{array}{ccc} K & \hookrightarrow & L \\ \uparrow & & \uparrow \\ A & \longrightarrow & B \end{array}$$

Basic properties

Integrality is stable under the ring operations: one would like the integrality of a and b to imply the integrality of $a + b$ and ab. This does hold, and we will be able to see it once we recast the notion of integrality in terms of commutative algebra.

Lemma 1.2.14. *Let* $A = (a_{ij})$ *be an* $r \times r$ *matrix over a ring* R*, and let*

$$A^* = (a_{ij}{}^*) = ((-1)^{i+j} \det A_{ij})$$

be the cofactor matrix of A*. Writing* Δ *for* $\det A$*,*

$$AA^* = A^*A = \Delta I_r$$

which implies that, given $x = (x_1, \ldots, x_r)$*,*

$$Ax = 0 \implies \Delta x = 0.$$

Theorem 1.2.15 (Integrality and finiteness)**.** *A finite number of* b_i *are integral over* $A \iff$ *the ring* $A[b_1, \dots, b_n]$ *is finitely generated as an* A*-module.*

Proof. Let $b \in B$ be integral over A, with $\beta(x) \in A[x]$ a monic polynomial of degree n satisfying $\beta(b) = 0$. For arbitrary $f \in A[x]$, we can use the division algorithm in $A[x]$ to get

$$f = g\beta + r,$$

where $\rho := \deg r < n$. Then

$$f(b) = g(b)\beta(b) + r(b) = r(b) = a_\rho b^\rho + \cdots + a_0$$

so $A[b]$ is generated as an A-module by $1, b, \dots, b^\rho$.

For the converse, let B be a finitely generated A-module with generators $t_1, \dots, t_n$. Any $\lambda \in B$ satisfies

$$\lambda t_i = \sum_j a_{ij} t_j$$

for some coefficients $a_{ij} \in A$. Writing $A = (a_{ij})$ and $t = (t_1, \dots, t_r)$, $(\lambda t_1, \dots, \lambda t_r) = \lambda t$ and

$$\left(\sum_j a_{1j} t_j, \cdots, \sum_j a_{rj} t_j \right) = At$$

which gives

$$(\lambda I_r - A)t = 0$$

implying, by our lemma, that

$$\det(\lambda I_r - A) \cdot t_i = 0 \tag{1.7}$$

for all i. Now, we know that the t_i form a generating set, so, in particular, 1 can be written as a linear combination of the t_i. This allows us to combine the system of equations 1.7 into

$$\det(\lambda I_r - A) = 0$$

which is a monic equation for λ over A. (Isn't this $\chi_A(\lambda)$?) ∎

Corollary 1.2.16. *If* a *and* b *are integral over* A*, so are* $a + b$ *and* ab*.*

Theorem 1.2.17 (Integrality is transitive)**.** *Consider ring extensions* $A \subseteq B \subseteq C$*.* $A \subseteq B$ *integral and* $B \subseteq C$ *integral* $\iff A \subseteq C$ *integral.*

Proof. $A \subseteq C$ integral implies $A \subseteq B$ integral, since every element of B is an element of C. Similarly, since every element $c \in C$ satisfies a monic polynomial in $A[x]$ and $A[x] \subseteq B[x]$, it also implies $B \subseteq C$ integral. Hence the integrality of the composite extension $A \subseteq C$ implies that the subextensions are also integral.

Conversely, let $c \in C$ satisfy

$$c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0$$

where $b_i \in B$. Let $R = A[b_1, \cdots, b_n]$. Then $R \subseteq R[c]$ is finite since c is integral over A, and $A \subseteq R$ is finite since $A \subseteq B$ is. Hence the composite extension $A \subseteq R[c]$ is finitely generated as an A-module and is thus integral. ∎

Theorem 1.2.18. *Any element* $l \in L$ *can be expressed as* b/a *for some* $b \in B$ *and* $a \in A$*.*

Proof. Consider an element $l \in L$. The minimal polynomial m_l of l over K gives rise to a polynomial over A

$$a_n l^n + a_{n-1} l^{n-1} + \cdots + a_0 = 0$$

by clearing denominators. Now observe that $\ell := a_n l$ is integral over A: multiplying by a_n^{n-1} gives an equation of the form

$$\ell^n + a'_{n-1}\ell^{n-1} + \cdots + a'_0 = 0.$$

This shows that taking $b/a = \ell/a_n$ works. ∎

Remark 1.2.19. Notice that $K(B) = L$. Indeed, $B \subset L$ so $K(B) \subset L$, and the result above shows that $L \subset K(B)$ (set-theoretically, $L \subset B \times A \subset B \times B$).

Theorem 1.2.20. *$l \in L$ is integral over A iff its minimal polynomial μ_l over K has coefficients in A.*

Proof. If $\mu := \mu_l \in A[x]$ then the integrality of l over A follows from the definition. Consider now the case of an integral l with minimal polynomial $\mu \in K[x]$. From integrality over A we know that l is a root of some $g \in A[x]$. Then $\mu \mid g$ in $K[x]$, so all zeros of μ are zeros of g and hence integral over A.

By Vietà, the coefficients a_i are given by elementary symmetric polynomials in the roots and are hence, by Theorem 1.2.16, integral over A themselves. The a_i are elements of K, so, in this case, integrality over A means that $a_i \in K$, and hence $\mu \in A[x]$. ∎

1.3 The trace and the norm

Given $x \in L$, multiplication by x determines an endomorphism

$$T_x : \alpha \mapsto x\alpha$$

of the K-vector space L. We define the trace and norm maps

$$\begin{aligned} \mathrm{Tr}_{L \mid K}(z) &= \mathrm{tr}\, T_z \\ \mathrm{Nm}_{L \mid K}(z) &= \det T_z \end{aligned}$$

Let $n = [L : K]$. The characteristic polynomial

$$\begin{aligned} \chi_z(t) &= \det(tI - T_z) \\ &= t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n \in K[i] \end{aligned}$$

contains coefficients $a_1 = \mathrm{Tr}_{L \mid K}(z)$ and $a_n = \mathrm{Nm}_{L \mid K}(z)$.

Remark 1.3.21. If this isn't immediately clear, think Vietà. (This will be one of the recurring themes throughout this chapter.)

1.4 Galois-theoretic interpretations

Fix an algebraic closure $\bar{K} = K^{alg}$ of K.

Proposition 1.4.22. *If $L \mid K$ is separable, letting $\sigma : L \to \bar{K}$ vary over the K-embeddings of L into $\bar{K}$, we have*

1. $\chi_z(t) = \prod_\sigma (t - \sigma z)$
2. $\mathrm{Tr}_{L \mid K}(z) = \sum_\sigma \sigma z$
3. $\mathrm{Nm}_{L \mid K}(z) = \prod_\sigma \sigma z$

Proof. Let $d = [L : K(x)]$. The characteristic polynomial is a power

$$\chi_z = \mu_z^d$$

where $d = [L : K(z)]$. Part 1 easily implies the others, by Vietà's formulas. ∎

Theorem 1.4.23. *For a tower of finite extensions $K \subseteq L \subseteq M$, we have*

$$\begin{aligned} \mathrm{Tr}_{L \mid K} \circ \mathrm{Tr}_{M \mid L} &= \mathrm{Tr}_{M \mid K} \\ \mathrm{Nm}_{L \mid K} \circ \mathrm{Nm}_{M \mid L} &= \mathrm{Nm}_{M \mid K} \end{aligned}$$

1.5 Integral bases

Definition 1.5.24. The *discriminant* of a basis α_i of a separable extension $L \mid K$ is defined by

$$d(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i \alpha_j))^2$$

where the σ_i are the K-embeddings $L \hookrightarrow \bar{K}$.

Proposition 1.5.25. *For $L \mid K$ a separable extension with basis α_i, the function*

$$(x, y) = \mathrm{Tr}_{L \mid K}(xy)$$

yields a nondegenerate bilinear form on the K-vector space L.

Corollary 1.5.26. *For $L \mid K$ and α_i as above,*

$$d(\alpha_1, \ldots, \alpha_n) \neq 0.$$

Proof. The form has matrix

$$M = \mathrm{Tr}_{L \mid K}((\alpha_i \alpha_j))$$

with respect to the given basis. The nondegeneracy of the form, which we have from Theorem 1.5.25, is equivalent to the statement that $\det M \neq 0$, whence the claim follows. ∎

Lemma 1.5.27. *Let (α_i) be a basis of $L \mid K$ contained in B, with $d = d(\alpha_1, \ldots, \alpha_n)$. Then*

$$dB \subseteq A\alpha_1 + \cdots + A\alpha_n.$$

Proposition 1.5.28. *If $L \mid K$ is separable and A is a PID, every finitely generated B-submodule $M \neq 0$ of L s a free A-module of rank $[L : K]$.*

Corollary 1.5.29. *B admits an integral basis over A.*

Proposition 1.5.30. *Let $M \mid K$ and $N \mid K$ be two Galois extensions with $M \cap N = K$, with $m = [M : K]$ and $n = [N : K]$. Fix integral bases $(\alpha_i)_{1 \leqslant i \leqslant m}$ of $M \mid K$ and $(\beta_j)_{1 \leqslant j \leqslant n}$ of $N \mid K$ respectively, with discriminants μ and ν respectively. If μ and ν are relatively prime, with $x\mu + y\nu = 1$ for some $x, y \in A$, then $(\alpha_i \beta_j)$ is an integral basis of MN, with discriminant $m^\nu n^\mu$.*

Proposition 1.5.31. *If $i \subseteq j$ are two nonzero finite $\mathcal{O}_K$-submodules of K, then $(j : i)$ is finite. Moreover,*

$$d(i) = (j : i)^2 d(j)$$

holds.

Appendix A

Commutative algebra

A.1 Rings

Proposition A.1.1. *The preimage of a prime ideal is also a prime ideal: given a ring map* $\phi : A \to B$ *and a prime ideal* $I \subset B$, $\phi^{-1}(I) \subset A$ *is also prime.*

Proof. Let $J = \phi^{-1}(I)$, and consider $xy \in J$. Then $\phi(xy) = \phi(x)\phi(y) \in I$, so either $\phi(x) \in I$ or $\phi(y) \in I$, which in turn tells us that either $x \in J$ or $y \in J$. ■

Proposition A.1.2. *The surjective image of a prime ideal is also a prime ideal: given a surjective ring morphism* $\sigma : A \twoheadrightarrow B$ *and a prime ideal* $I \subset A$, $\sigma(I) \subset B$ *is also prime.*

Proof. This is a simple variant of the argument for Theorem A.1.1. Let $J = \sigma(I)$, and consider $xy \in J$. By surjectivity, there exist a and b such that

$$\sigma(a) = x$$
$$\sigma(b) = y$$

yielding $\sigma(ab) = xy$. Then $ab \in I$, which implies that (wlog) $a \in I$ since I is prime. Then $\sigma(a) = x \in J$, so that J is also prime. ■

Proposition A.1.3. *Let* I *be an ideal of* A*. Consider the natural map*

$$\pi : A \to A/I.$$

Then π^{-1} *gives an inclusion-preserving bijection between prime ideals of* A/I *and prime ideals of* A *containing* I*.*

Proof. This is one form of the third isomorphism theorem (TODO REF).

For one inclusion, we apply Theorem A.1.1, noting that (after convincing oneself that the map preserves inclusions) the preimage of a prime ideal $P \subset A/I$ must contain I since $(0) \subset P$ and $\pi^{-1}((0)) = I$. TODO ■

Proposition A.1.4. *The map* $\phi : k[x] \to k[x, \epsilon]/(\epsilon^2)$ *sending* $x \mapsto x + \epsilon$ *maps*

$$f(x) \mapsto f(x) + \epsilon f'(x).$$

A.2 Tensor products of modules

A.3 Operations on modules

A.4 Localization