Elementary Number Theory II

David Pierce

Spring 2008
Edited January 5, 2018

Matematik Bölümü
Mimar Sinan Güzel Sanatlar Üniversitesi
dpierce@msgsu.edu.tr
http://mat.msgsu.edu.tr/~dpierce/

Preface

These are notes from Elementary Number Theory II (Math 366) in the Mathematics Department of Middle East Technical University, Ankara, spring semester, 2007-8. The catalogue description was,

> Arithmetic in Quadratic fields. Factorization theory, Continued fractions, Periodicity. Transcendental numbers.

Class met Tuesdays at 13:40 for two hours and Fridays at 13:40 (originally 12:40) for one hour. I typeset the notes after class, relying on memory and the handwritten notes that I had prepared before class. I did some polishing, correcting, and rearrangement. Now, ten years later, I have done some more.

The main published reference for the course was Adams and Goldstein [1], which had apparently been on reserve in the library since the last time the course had offered, several years earlier. I had that text only in the form of a photocopy of chapters 6–11, used by Ayşe Berkman when she was a student. The text was a rough guide only.

Special symbols used in these notes are found at the head of the index.

For continued fractions, the Burton text [4] used for Math 365 is useful, as are Hardy and Wright [6] and Shockley [10]. I also consulted Everest and Ward [5], Landau [8], and occasionally other works.

Class was cancelled Friday, February 29, 2008 because I was in Istanbul for my *doçentlik* exam. Ayşe taught for me on the following Tuesday, since I was sick with a gastro-intestinal infection from the trip. I was sick again, with the flu, on May 13 and 16; class was cancelled.

There were examinations on the Mondays March 24, April 28, and May 26, so there were no lectures covering new material on the previous Fridays.

Class on Tuesday, April 8, was only one hour, because of a special seminar that day (on teaching conic sections).

The chapter for April 22 is a reworking of what I presented vaguely and incorrectly in class. Theorem 28 was not given at all in class.

The notes were formatted originally for A4 paper; I have now changed over to A5, which allows whole pages—even two pages, side by side—to be read in a computer screen.

I have also edited the mathematical presentation. I have added the overview on page 11, the summary on page 72, and just after this, Theorem 16, which can now be appealed to in Problem 7.

I had originally used both $\mathbb{N}$ and ω for the set $\{0, 1, 2, \dots\}$ of natural numbers; now only ω is used. I have decided that, if one wants a symbol for the set $\{1, 2, 3, \dots\}$ of counting numbers, this is where $\mathbb{N}$ should be used.

Contents

Conventions **9**

1. February 19, 2008 (Tuesday) **11**
Diophantine equations 11
Pythagorean triples 11
Infinite descent 13

2. February 22, 2008 (Friday) **18**
Rational points of the circle 18
Continued fractions 20

3. February 26, 2008 (Tuesday) **24**
Euclidean algorithm 24
Pell equation 29

4. March 4, 2008 (Tuesday) **33**
Quadratic fields 33
Gaussian integers 35

5. March 7, 2008 (Friday) **37**
Euclidean domains 37

6. March 11, 2008 (Tuesday) **40**
Unique-factorization domains 40
Gaussian primes 41
Arbitrary quadratic fields 45

7. March 14, 2008 (Friday) **48**
Quadratic forms 49

8. March 18, 2008 (Tuesday) **54**
Lattices and elliptic curves 54
Quadratic lattices 56
Pell equation examples 57

9. March 25, 2008 (Tuesday) **61**
Quadratic form example 61
Discriminants 62
Quadratic form example 64
Lattices 66

10. March 28, 2008 (Friday) **68**
Orders and conductors 68

11. April 1, 2008 (Tuesday) **71**
Units 72
Imaginary case 73
Real case 80

12. April 4, 2008 (Friday) **83**
Golden ratio 83

13. April 8, 2008 (Tuesday) **85**
Real example 85

14. April 11, 2008 (Friday) **89**
Example continued 89

15. April 15, 2008 (Tuesday) **93**
Units from convergents 93

16. April 18, 2008 (Friday) **99**
The cases of 13 and 5 99

17. April 22, 2008 (Tuesday) **103**
Continued fractions 103

18. April 29, 2008 (Tuesday) **112**
Norm of a lattice 112

19. May 2, 2008 (Friday) **117**
Products of lattices 117

20. May 6, 2008 (Tuesday) **120**
Arithmetic of lattices 120

21. May 9, 2008 (Friday) **124**
Prime factorizations 124

22. May 20, 2008 (Tuesday) **127**
Primes 127

A. Exercises **130**
A.1. February 26, 2008 130
A.2. March 11, 2008 131
A.3. April 3, 2008 132
A.4. April 10, 2008 133
A.5. May 18, 2008 134

B. Examinations **136**
B.1. March 24, 2008 (Monday) 136
B.2. May 26 (Monday) 141
B.3. June 2, 2008 (Monday) 147

Bibliography **150**

Index **152**

List of Figures

2.1. Rational points of the circle 19
5.1. A lattice of Gaussian multiples 38
6.1. Estimating the area of a circle 44
7.1. Lattice and isomorphic sublattice 53
8.1. A fundamental parallelogram of a lattice 54
8.2. An elliptic curve 55
10.1. Lattices $\langle 1, \mathrm{i}/\sqrt{a}\rangle$ 69
10.2. Lattices $\langle 1, (1+\mathrm{i}\sqrt{4a-1})/2a\rangle$ 70
11.1. Units in imaginary quadratic fields 74
11.2. Ellipse $\frac{1}{3}\left(x+\frac{1}{2}y\right)^2+\frac{1}{4}y^2=1$ 75
11.3. Solutions of $x^2+xy+y^2=3$ 76
11.4. Solutions of $\mathrm{N}(\xi)=3$ from $\langle 1,\omega\rangle$ in $\mathbb{Q}(\sqrt{-3})$ . . 77
11.5. Ellipse $\frac{3}{7}x^2+\frac{1}{7}(x+y)^2=1$ 78
11.6. Solutions to $4x^2+2xy+1=7$ 78
11.7. Subfields of $\mathbb{Q}(\sqrt{3},\mathrm{i})$ 79
11.8. Solutions of $\mathrm{N}(\xi)=7$ from $\langle 1,2\omega\rangle$ in $\mathbb{Q}(\sqrt{-3})$. 80
13.1. Hyperbola $(2x+\frac{1}{2}y)^2-\frac{5}{4}y^2=4$ 86
13.2. Small solutions of $4x^2+2xy-y^2=4$ 88
14.1. Solutions of $4x^2+2xy-y^2=4$ 90
18.1. Lattices $\langle 1,\mathrm{i}\rangle$ and $\langle 3, 1+2\,\mathrm{i}\rangle$ 115
21.1. Index-2 sublattices of $\langle 1,\sqrt{-5}\rangle$ 125
B.1. Solutions of $\mathrm{N}(\xi)=19$ from $\langle 1,2\omega\rangle$ in $\mathbb{Q}(\sqrt{-3})$ 143

List of Tables

14.1. Solutions of $4x^2 + 2xy - y^2 = 4$ 91
16.1. Convergents and units when $d = 13$ 100

Conventions

- In the Pell equation $x^2 - dy^2 = 1$ (namely (3.6), page 29), d is a positive non-square (pages 29 and 103).
- K is a quadratic field (page 33).
- K is more precisely the field $\mathbb{Q}(\sqrt{d})$, where d is now a square-free integer, possibly negative, different from 1 (page 45).
- $(a + b\sqrt{d})' = a - b\sqrt{d}$ in K ((6.3), page 45).
- $\mathrm{N}(\alpha) = \alpha\alpha'$ ((4.2), page 36).
- $\mathfrak{O}_K$ is the set of integers of K (page 46).
- $\omega = \left\{ \begin{array}{ll} \sqrt{d}, & \text{if } d \equiv 2 \text{ or } 3 \pmod 4 \\ \dfrac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod 4 \end{array} \right\}$ (page 48).
- $\mathfrak{O}_K$ is the ring $\mathbb{Z}[\omega]$ by Theorem 11 (page 48).
- α and β are elements of K (page 56).
- D is the discriminant of a quadratic form (pages 50–65), either
  - $b^2 - 4ac$ when the form is $ax^2 + bxy + cy^2$ ((7.3), page 49)), or
  - $\begin{vmatrix} \alpha & \alpha' \\ \beta & \beta' \end{vmatrix}^2$ when the form is $\mathrm{N}(\alpha x + \beta y)$ ((9.3), 63).

- Λ is the lattice $\mathbb{Z}\alpha \oplus \mathbb{Z}\beta$ (page 51).
- $\mathrm{End}(\Lambda)$ is the ring of endomorphisms of Λ (page 51).
- $\Delta(\Lambda)$ is the discriminant $\begin{vmatrix}\alpha & \alpha' \\ \beta & \beta'\end{vmatrix}^2$ of Λ ((9.4) and pages 64–116).
- $\mathfrak{O}_\Lambda$ is $\mathrm{End}(\Lambda)$ (page 68).
- $\mathfrak{O}_\Lambda = \langle 1, c\omega \rangle$ for some c (Theorem 12, page 68), the conductor of $\mathfrak{O}_\Lambda$.
- We may assume Λ is the lattice $\langle 1, \tau \rangle$, where $\tau = \beta/\alpha$ and also $a\tau^2 = -b\tau - c$ for some rational integers a, b, and c with no common nontrivial factor (page 69).
- ε_Λ is the fundamental unit of $\mathfrak{O}_\Lambda$ (page 81).

1. February 19, 2008 (Tuesday)

Diophantine equations

We shall be solving some **Diophantine equations,** that is, polynomial equations in which all constants and variables are integers.

- The solution of the Fermat equation $x^4+y^4 = z^4$ or (1.2) in Problem 2 is that there is no solution.
- A solution of (1.2) *would* provide a solution of the Pythagorean equation $x^2 + y^2 = z^2$ or (1.1) in Problem 1.
- Restricting ourselves to two variables, we solve the equations of the form $x^2 + y^2 = n$ or (1.4) in Problem 3.

As illustrations of a general method, we give solutions of

- $x^2 - 14y^2 = 1$ or (8.1) in Problem 5 (page 57);
- $x^2 + xy + y^2 = 3$ or (11.5) in Problem 6 (page 74);
- $4x^2 + 2xy + y^2 = 7$ or (11.7) in Problem 7 (page 76);
- $4x^2 + 2xy - y^2 = 4$ or (13.1) in Problem 8 (page 85).

The method will involve passing to *quadratic extensions* of the field $\mathbb{Q}$ of rational numbers.

Pythagorean triples

Problem 1. *Solve (that is, find all solutions of)*

$$x^2 + y^2 = z^2, \tag{1.1}$$

Solution. The following are equivalent:

(i) (a, b, c) is a solution;
(ii) $(|a|, |b|, |c|)$ is a solution;
(iii) (na, nb, nc) is a solution for all nonzero n;
(iv) (b, a, c) is a solution.

Also, (1.1) is equivalent to

$$x^2 = (z + y)(z - y).$$

Suppose (a, b, c) is a solution of (1.1) such that $a, b, c > 0$ and $\gcd(a, b, c) = 1$. Then (a, b, c) may be called a **primitive solution,** and all solutions can be obtained from primitive solutions. Observe that not both a and b are even. Also, if $a, b \equiv 1 \pmod 2$, then $c^2 \equiv a^2 + b^2 \equiv 2 \pmod 4$, which is absurd. So exactly one of a and b is even. Say a is even. Then b and c are odd, and

$$\left(\frac{a}{2}\right)^2 = \left(\frac{c+b}{2}\right)\left(\frac{c-b}{2}\right).$$

Also $(c+b)/2$ and $(c-b)/2$ are co-prime, since their sum is c and their difference is b. Hence each must be a square; say

$$\frac{c+b}{2} = n^2, \qquad \frac{c-b}{2} = m^2,$$

where $n, m > 0$. Then

$$c = n^2 + m^2, \qquad b = n^2 - m^2, \qquad a = 2nm.$$

Moreover, n and m are co-prime, and exactly one of them is odd (since c is odd).

Conversely, suppose n and m are co-prime, exactly one of them is odd, and $0 < m < n$. Then the triple $(2nm, n^2 - m^2, n^2 + m^2)$ solves (1.1). Moreover, every common prime

factor of $n^2 - m^2$ and $n^2 + m^2$ is a factor of the sum $2n^2$ and the difference $2m^2$, and is odd, so it is a common factor of n and m. Thus there is no common prime factor, and the triple is a *primitive* solution.

We conclude that there is a one-to-one correspondence between:

(i) pairs (m, n) of co-prime integers, where $0 < m < n$, and exactly one of m and n is odd;

(ii) primitive solutions (a, b, c) to (1.1), where a is even.

The correspondence is $(x, y) \mapsto (2xy, y^2 - x^2, y^2 + x^2)$. □

Infinite descent

Problem 2. *Solve*

$$x^4 + y^4 = z^4. \tag{1.2}$$

Solution. Let (a, b, c) be a solution, where $a, b, c > 0$, and $\gcd(a, b, c) = 1$. Then (a^2, b^2, c^2) is a primitive **Pythagorean triple,** that is, a solution to (1.1). We may assume a is even, and so

$$a^2 = 2mn, \qquad b^2 = n^2 - m^2, \qquad c^2 = n^2 + m^2$$

for some positive m and n. In particular,

$$m^2 + b^2 = n^2.$$

Since $\gcd(a, b) = 1$, and every prime factor of m divides a, we have $\gcd(m, b) = 1$. Hence (m, b, n) is a primitive Pythagorean triple. Also m is even, since b is odd. Hence

$$m = 2de, \qquad b = e^2 - d^2, \qquad n = e^2 + d^2$$

for some d and e. Then

$$a^2 = 2mn = 4de(e^2 + d^2).$$

But $\gcd(d, e) = 1$, so e^2+d^2 is prime to both d and e. Therefore each of d, e, and $e^2 + d^2$ must be square: say

$$d = r^2, \qquad e = s^2, \qquad e^2 + d^2 = t^2.$$

This gives $t^2 = e^2 + d^2 = s^4 + r^4$; that is, (s, r, t) is a solution to

$$x^4 + y^4 = z^2. \tag{1.3}$$

But (a, b, c^2) is also a solution to this; moreover,

$$1 \leqslant |t| \leqslant t^2 = e^2 + d^2 = n \leqslant n^2 < n^2 + m^2 = c^2.$$

We never used that c^2 is a square. Thus, for every solution to (1.3) with positive entries, there is a solution with positive entries in which the third entry is smaller. This is absurd; therefore there is no such solution to (1.3), or to (1.2). □

We used here Fermat's method of **infinite descent.**

In Elementary Number Theory I, we proved that the Diophantine equation

$$x^2 + y^2 + z^2 + w^2 = n$$

is soluble for every positive integer n.

Problem 3. *Find those n for which*

$$x^2 + y^2 = n \tag{1.4}$$

is soluble.

Solution. Let S be the set of such n. Since

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= |a+b\,\mathrm{i}\,|^2|c+d\,\mathrm{i}\,|^2\\ &= |(a+b\,\mathrm{i}\,)(c+d\,\mathrm{i}\,)|^2\\ &= |(ac-bd)+(ad+bc)\,\mathrm{i}\,|^2\\ &= (ac-bd)^2+(ad+bd)^2,\end{aligned}$$

S is closed under multiplication. We ask now: Which primes are in S?

All squares are congruent to 0 or 1 *modulo* 4. Hence elements of S are congruent to 0, 1, or 2 *modulo* 4. Therefore S contains no primes that are congruent to 3 (mod 4). However, S does contain 2, since $2 = 1^2 + 1^2$.

Suppose conversely $p \equiv 1 \pmod 4$. We shall show $p \in S$. We have that -1 is a quadratic residue *modulo* p, so

$$-1 \equiv a^2 \pmod p$$

for some a, where we may assume $|a| < p/2$. Hence

$$a^2 + 1 = tp$$

for some positive t. In particular, $tp \in S$. Also,

$$0 < t = \frac{a^2+1}{p} < \frac{(p/2)^2+1}{p} = \frac{p}{4} + \frac{1}{p} < p.$$

Thus, letting k be simply the least positive t such that $tp \in S$, we have $0 < k < p$. By definition,

$$kp = b^2 + c^2 \tag{1.5}$$

for some b and c. There are d and e such that

$$d \equiv b \;\&\; e \equiv c \pmod k, \qquad |d|, |e| \leqslant \frac{k}{2}.$$

Then $d^2 + e^2 \equiv b^2 + c^2 \equiv 0 \pmod{k}$, so

$$d^2 + e^2 = km \tag{1.6}$$

for some m, where

$$0 \leqslant m = \frac{d^2 + e^2}{k} \leqslant \frac{2(k/2)^2}{k} = \frac{k}{2} < k.$$

But multiply (1.5) and (1.6), getting

$$k^2 mp = (b^2 + c^2)(d^2 + e^2) = (bd + ce)^2 + (be - cd)^2.$$

We can divide by k^2, since

$$bd + ce \equiv b^2 + c^2 \equiv 0 \;\; \& \;\; be - cd \equiv bc - cb \equiv 0 \pmod{k}.$$

Thus we obtain

$$mp = \left(\frac{bd + ce}{k}\right)^2 + \left(\frac{be - cd}{k}\right)^2.$$

This implies $mp \in S$. By minimality of k, we have $m = 0$. Therefore $d^2 + e^2 = 0$, so $d = 0 = e$. Then $b, c \equiv 0 \pmod{k}$, so

$$k^2 \mid kp,$$

and therefore $k \mid p$. This means $k = 1$, so $p \in S$.

Finally, suppose $n \in S$ and $p \mid n$. Then $n = a^2 + b^2$ for some a and b, so

$$a^2 + b^2 \equiv 0 \pmod{p}.$$

If $p \mid a$, then $p \mid b$, so $p^2 \mid n$, which means n is not square-free. If $p \nmid a$, then a is invertible *modulo* p, so $1 + (b/a)^2 \equiv 0 \pmod{p}$, which means -1 is a quadratic residue *modulo* p, and so $p = 2$ or else $p \equiv 1 \pmod{4}$.

The conclusion is that S contains just those numbers of the form $n^2 m$, where m is square-free and has no prime factors congruent to 3 *modulo* 4. □

We shall develop an alternative solution by means of Theorem 7 on page 41. This will let us count the solutions of (1.4) as in Theorem 8, and *this* will give us the series for π in Theorem 9.

2. February 22, 2008 (Friday)

Rational points of the circle

Solving (1.1) in integers is related to integrals like

$$\int \frac{\mathrm{d}\,\theta}{2+3\sin\theta},$$

which one can solve by the substitution

$$t = \tan\frac{\theta}{2}, \qquad \mathrm{d}\,t = \frac{1}{2}\sec^2\frac{\theta}{2}\,\mathrm{d}\,\theta,$$

so that

$$\sin\theta = \frac{2t}{1+t^2}, \qquad \cos\theta = \frac{1-t^2}{1+t^2}, \qquad \mathrm{d}\,\theta = \frac{2\,\mathrm{d}\,t}{1+t^2}.$$

Concerning (1.1), we have

$$x^2+y^2=z^2 \iff \left(\frac{x}{z}\right)^2+\left(\frac{y}{z}\right)^2 = 1 \text{ or } x=y=z=0.$$

So finding Pythagorean triples corresponds to solving

$$x^2+y^2=1$$

in *rationals*. To do so, since the equation defines the unit circle, consider also the line through $(-1,0)$ with slope t, so that its Y-intercept is also t, as in Figure 2.1: this line is given by

$$y = tx + t. \tag{2.1}$$

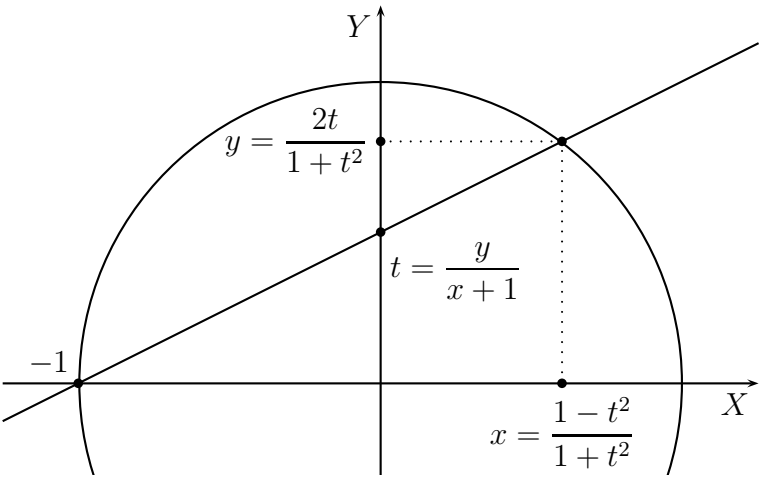

Figure 2.1.: Rational points of the circle

The circle and the line meet at $(-1, 0)$ and also (x, y), where

$$\begin{aligned} x^2 + (tx + t)^2 &= 1, \\ (1 + t^2)x^2 + 2t^2x + t^2 - 1 &= 0, \\ x^2 + \frac{2t^2}{1 + t^2} \cdot x - \frac{1 - t^2}{1 + t^2} &= 0. \end{aligned}$$

The constant term in the left member of the last equation is the product of the roots; one of the roots is -1; so we get

$$(x, y) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right).$$

If t is rational, then so are the coordinates of this point, which is therefore a **rational point** of the circle. Conversely, if x and y are rational, then so is t, by (2.1). Hence the function

$$t \mapsto \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right)$$

is a one-to-one correspondence, with inverse

$$(x, y) \mapsto \frac{y}{x+1},$$

between $\mathbb{Q}$ and the set of rational points, other than $(-1, 0)$, of the unit circle.

Hence we can conclude that every integral solution of (1.1) is a multiple of

$$(1 - t^2, 2t, 1 + t^2).$$

Taking $t = m/n$ and multiplying by n^2, we get

$$(n^2 - m^2, 2mn, n^2 + m^2),$$

the solution we found before.

Continued fractions

We can convert $\sqrt{2}$ into a *continued fraction* as follows. First

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{\left(\frac{1}{\sqrt{2}-1}\right)} = 1 + \frac{1}{\sqrt{2}+1}.$$

Note that $0 < \sqrt{2} - 1 < 1$. We now have

$$\sqrt{2} + 1 = 2 + \frac{1}{\sqrt{2}+1},$$

so we can substitute repeatedly:

$$\sqrt{2} = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{2 + \frac{1}{\sqrt{2}+1}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{2}+1}}}$$

and so on. In the general procedure, given a real number x, we first write

$$x = a_0 + \xi_0,$$

where

$$a_0 = [x], \qquad \xi_0 = x - a_0, \tag{2.2}$$

square brackets denoting the greatest-integer function. Now

$$\xi_0 = \frac{1}{\left(\dfrac{1}{\xi_0}\right)} = \frac{1}{a_1 + \xi_1},$$

$$a_1 = \left[\frac{1}{\xi_0}\right], \qquad \xi_1 = \frac{1}{\xi_0} - a_1. \tag{2.3}$$

We continue recursively, letting

$$a_n = \left[\frac{1}{\xi_{n-1}}\right], \qquad \xi_n = \frac{1}{\xi_{n-1}} - a_n, \tag{2.4}$$

where ξ_{n-1} must be non-zero for a_n to be defined. Then

$$x = a_0 + \xi_0 = a_0 + \frac{1}{a_1 + \xi_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \xi_2}}$$

and so on. We thus obtain **continued fractions** for x. For example, when $x = \sqrt{3}$, we get

$$\begin{aligned}
& & a_0 = 1, \qquad & \xi_0 = \sqrt{3} - 1, \\
\frac{1}{\xi_0} = \frac{\sqrt{3}+1}{2}, \qquad & & a_1 = 1, \qquad & \xi_1 = \frac{\sqrt{3}-1}{2}, \\
\frac{1}{\xi_1} = \sqrt{3} + 1, \qquad & & a_2 = 2, \qquad & \xi_2 = \sqrt{3} - 1,
\end{aligned}$$

and now the process repeats:

$$\xi_n = \begin{cases} \sqrt{3}-1, & \text{if } n \text{ is even;} \\ \dfrac{\sqrt{3}-1}{2}, & \text{if } n \text{ is odd;} \end{cases}$$

$$a_n = \begin{cases} 1, & \text{if } n = 0, \text{ or } n \text{ is odd;} \\ 2, & \text{if } n \text{ is positive and even.} \end{cases}$$

It appears that

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}}. \tag{2.5}$$

If this has any meaning though, it should be that $\sqrt{3}$ is the *limit*, in the sense of calculus, of the sequence

$$1, \qquad 1 + \frac{1}{1}, \qquad 1 + \cfrac{1}{1 + \cfrac{1}{2}}, \qquad 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1}}}, \qquad \dots$$

We introduce some notation for the terms of this sequence. Here square brackets do *not* denote the greatest-integer function:

$$[a_0] = a_0, \quad [a_0; a_1] = a_0 + \frac{1}{a_1}, \quad [a_0; a_1, a_2] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}},$$

and so forth; the general term is given recursively by

$$[a_0; a_1, \ldots, a_{n+1}] = \left[a_0; a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right]. \qquad (2.6)$$

Here we must have $a_n \neq 0$ when $n > 0$; we shall assume also $a_n > 0$ when $n > 0$. We can also use the notation in the infinite case. For example, from $\sqrt{3}$, we have obtained $[1; 1, 2, 1, 2, \ldots]$, which we can write as

$$[1; \overline{1, 2}].$$

We have not yet proved that this is the limit of the sequence

$$[1], \quad [1; 1], \quad [1; 1, 2], \quad [1; 1, 2, 1], \quad [1; 1, 2, 1, 2], \quad \ldots.$$

3. February 26, 2008 (Tuesday)

Euclidean algorithm

Obtaining the sequences $(a_n : n \in \omega)$ and $(\xi_n : n \in \omega)$ from x as above corresponds to applying the **Euclidean algorithm.** With this algorithm, we find the greatest common divisor of 155 and 42 by computing

$$\begin{aligned} 155 &= 42 \cdot 3 + 29, \\ 42 &= 29 \cdot 1 + 13, \\ 29 &= 13 \cdot 2 + 3, \\ 13 &= 3 \cdot 4 + 1. \end{aligned}$$

Since $1 \mid 3$, we have $\gcd(155, 42) = 1$, We are now interested in the sequence $(3, 1, 2, 4, 3)$ of multipliers, which is a sequence of greatest integers in fractions, obtained as follows.

$$\begin{aligned} \left[\frac{155}{42}\right] &= 3, & \frac{155}{42} - 3 &= \frac{29}{42}, \\ \left[\frac{42}{29}\right] &= 1, & \frac{42}{29} - 1 &= \frac{13}{29}, \\ \left[\frac{29}{13}\right] &= 2, & \frac{29}{13} - 2 &= \frac{3}{13}, \\ \left[\frac{13}{3}\right] &= 4, & \frac{13}{3} - 4 &= \frac{1}{3}, \end{aligned}$$

and finally $[3/1] = [3] = 3$. In short, the sequence $(3, 1, 2, 4, 3)$ is the sequence of a_n as defined earlier, when $x = 155/42$.

Moreover,

$$\frac{155}{42} = 3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{3}}}}.$$

In the same way, we can write every fraction as a (finite) **continued fraction** $[a_0; a_1, \ldots, a_n]$, where the a_k are integers, and all of them are positive except perhaps a_0. Such a continued fraction is called **simple.** We shall work only with simple continued fractions. But the continued fraction obtained for irrational x does not terminate.

The kth **convergent** of $[a_0; a_1, \ldots]$ is $[a_0; a_1, \ldots, a_k]$. For example, by a tedious computation to be made easier in a moment, the convergents of $[1; \overline{1, 2}]$ are

$$1, \quad 2, \quad \frac{5}{3}, \quad \frac{7}{4}, \quad \frac{19}{11}, \quad \frac{26}{15}, \quad \frac{71}{41}, \quad \frac{97}{56}, \quad \ldots$$

How are these convergents as approximations of $\sqrt{3}$? We check

a few of them:

$$\left(\frac{5}{3}\right)^2 = \frac{25}{9}, \qquad 25 - 3 \cdot 9 = -2,$$
$$\left(\frac{7}{4}\right)^2 = \frac{49}{16}, \qquad 49 - 3 \cdot 16 = 1,$$
$$\left(\frac{19}{11}\right)^2 = \frac{361}{121}, \qquad 361 - 3 \cdot 121 = -2,$$
$$\left(\frac{26}{15}\right)^2 = \frac{676}{225}, \qquad 676 - 3 \cdot 225 = 1,$$
$$\left(\frac{71}{41}\right)^2 = \frac{5041}{1681}, \qquad 5041 - 3 \cdot 1681 = -2.$$

If the pattern of differences continues, and the denominators of the convergents grow without bound, then indeed the convergents converge to $\sqrt{3}$.

In general, we shall write the kth convergent of $[a_0; a_1, \dots]$ as p_k/q_k. However, this does not define p_k and q_k separately, unless we require them to be positive and prime to one another. We shall take a different route; p_k and q_k will be prime to one another, but not by definition. Since we want $p_0/q_0 = a_0$, we just define

$$p_0 = a_0, \qquad q_0 = 1. \tag{3.1}$$

Since we want $p_1/q_1 = [a_0; a_1]$, and now

$$[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_0 a_1 + 1}{a_1},$$

we define

$$p_1 = p_0 a_1 + 1, \qquad q_1 = a_1. \tag{3.2}$$

We want $p_2/q_1 = [a_0; a_1, a_2]$, and now

$$[a_0; a_1, a_2] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1} = \frac{p_1 a_2 + p_0}{q_1 a_2 + q_0},$$

so we define

$$p_2 = p_1 a_2 + p_0, \qquad q_2 = q_1 a_2 + q_0. \tag{3.3}$$

Following the pattern of (3.3), we define

$$p_{k+2} = p_{k+1} a_{k+2} + p_k, \qquad q_{k+2} = q_{k+1} a_{k+2} + q_k; \tag{3.4}$$

but now we have to check that this gives us what we want.

Theorem 1. *Under the definitions* (3.1), (3.2), *and* (3.4), *for all* k *in* ω,

$$\frac{p_k}{q_k} = [a_0; a_1, \ldots, a_k]. \tag{3.5}$$

Proof. We use induction. By design, the claim holds when k is 0, 1, or 2. Supposing, for some j in ω, the claim holds when $k = j + 2$, using the recursive definition (2.6), we have

$$\begin{aligned}
[a_0; a_1, \ldots, a_{j+3}] &= \left[a_0; a_1, \ldots, a_{j+1}, a_{j+2} + \frac{1}{a_{j+3}}\right] \\
&= \frac{p_{j+1} \cdot \left(a_{j+2} + \dfrac{1}{a_{j+3}}\right) + p_j}{q_{j+1} \cdot \left(a_{j+2} + \dfrac{1}{a_{j+3}}\right) + q_j} \\
&= \frac{p_{j+1} a_{j+2} a_{j+3} + p_{j+1} + p_j a_{j+3}}{q_{j+1} a_{j+2} a_{j+3} + q_{j+1} + q_j a_{j+3}} \\
&= \frac{p_{j+2} a_{j+3} + p_{j+1}}{q_{j+2} a_{j+3} + q_{j+1}} = \frac{p_{j+3}}{q_{j+3}}.
\end{aligned}$$

By induction, we have (3.5) for all k. □

We now confirm the additional property that we wanted.

Theorem 2. *For all k in ω,*

$$\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} = \frac{(-1)^k}{q_{k+1}q_k},$$

equivalently,

$$p_{k+1}q_k - p_k q_{k+1} = (-1)^k.$$

Proof. Again we use induction. From (3.1) and (3.2), we have

$$\frac{p_1}{q_1} - \frac{p_0}{q_0} = \frac{1}{a_1} = \frac{(-1)^0}{q_1 q_0},$$

so the claim holds when $k = 0$. Supposing it holds for some k, we have

$$\begin{aligned} p_{k+2}q_{k+1} - p_{k+1}q_{k+2} \\ &= (p_{k+1}a_{k+2} + p_k)q_{k+1} - p_{k+1}(q_{k+1}a_{k+2} + q_k) \\ &= p_k q_{k+1} - p_{k+1}q_k, \end{aligned}$$

which is $-(-1)^k$, that is, $(-1)^{k+1}$. Thus the claim holds for all k. □

Corollary. *The integers p_k and q_k are prime to one another, the sequences $\{p_{2n}/q_{2n}\}$ $\{p_{2n+1}/q_{2n+1}\}$ are respectively increasing and decreasing, and*

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

The two sequences converge to the same limit. If the convergents are obtained as above from x, then their limit is x.

Now we are justified in writing (2.5).

Pell equation

With these tools, we turn now to the **Pell equation,**

$$x^2 - dy^2 = 1. \tag{3.6}$$

We first take care of some trivial cases:

(i) If $d < -1$, then $(x, y) = (\pm 1, 0)$.
(ii) If $d = -1$, then (x, y) is $(\pm 1, 0)$ or $(0, \pm 1)$.
(iii) If $d = 0$, then $x = \pm 1$, while y is anything.
(iv) If d is a positive square, as a^2, the the equation becomes

$$(x + ay)(x - ay) = 1,$$

so $x \pm ay$ are equal to one another and to ± 1, and therefore $y = 0$ and $x = \pm 1$.

We assume d is a positive non-square

for the rest of this lecture (and again on page 103). Thus

$$d \in \{2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 17, \dots\}.$$

Then (3.6) still has the solution $(\pm 1, 0)$; but perhaps it has others too. Indeed, in case $d = 3$, on page 26 we found solutions $(49, 16)$ and $(676, 225)$, with a possibility of finding more if the pattern continued.

Suppose (a, b) and (s, t) are solutions to (3.6); This means

$$a^2 - db^2 = 1, \qquad s^2 - dt^2 = 1.$$

Multiplication gives

$$1 = (a^2 - db^2)(s^2 - dt^2) = (as \pm dbt)^2 - d(at \pm bs)^2, \tag{3.7}$$

and so each pair $(as \pm dbt, at \pm bs)$ is a solution.

We can repeat this process as follows, noting also

$$a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d}).$$

If we define (a_n, b_n) by

$$a_n + b_n\sqrt{d} = (a + b\sqrt{d})^n, \tag{3.8}$$

then also $a_n - b_n\sqrt{d} = (a - b\sqrt{d})^n$, so

$$a_n{}^2 - db_n{}^2 = (a + b\sqrt{d})^n(a - b\sqrt{d})^n = (a^2 - b^2d)^n = 1,$$

and (a_n, b_n) is a solution to (3.6). If $a + b\sqrt{d} > 1$, then these solutions (a_n, b_n) must all be distinct. We ask now whether there is even *one* solution (a, b) such that $a + b\sqrt{d} > 1$.

Lemma 1. *For some positive k, the equation*

$$x^2 - dy^2 = k \tag{3.9}$$

has infinitely many solutions.

Proof. Let $(p_n/q_n : n \in \omega)$ be the sequence of convergents for $\sqrt{d}$. When n is odd, we have

$$\begin{aligned} 0 < \frac{p_n}{q_n} - \sqrt{d} < \frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} = \frac{1}{q_{n+1}q_n} < \frac{1}{q_n{}^2}, \\ 0 < \frac{p_n}{q_n} + \sqrt{d} < \frac{2p_n}{q_n}; \end{aligned}$$

multiplying gives

$$0 < \frac{p_n{}^2}{q_n{}^2} - d < \frac{2p_n}{q_n{}^3}, \qquad 0 < p_n{}^2 - dq_n{}^2 < \frac{2p_n}{q_n} < \frac{2p_1}{q_1}.$$

Thus there are finitely many possibilities for $p_n{}^2 - dq_n{}^2$, so one of them must be realized infinitely many times. □

If (a, b) solves (3.6), and each of a and b is positive, then let us refer to (a, b) as a **positive** solution.

Lemma 2. (3.6) *has a positive solution.*

Proof. By the previous lemma, we may let k be a positive number such that (3.9) has infinitely many solutions. But there are just finitely many pairs (a, b) such that $0 \leqslant a < k$ and $0 \leqslant b < k$. Hence there must be one such pair for which (3.9) together with the congruences

$$x \equiv a, \quad y \equiv b \pmod{k}$$

have infinitely many solutions. Let (m, n) and (s, t) be two such solutions. Then by the identity in (3.7), we have

$$k^2 = (m^2 - dn^2)(s^2 - dt^2) = (ms - dnt)^2 - d(mt - ns)^2.$$

But we have also

$$ms - dnt \equiv m^2 - dn^2 \equiv 0, \quad mt - ns \equiv mn - nm \equiv 0 \pmod{k}.$$

So we can divide by k^2 to get

$$1 = \left(\frac{ms - dnt}{k}\right)^2 - d\left(\frac{mt - ns}{k}\right)^2.$$

Changing signs as needed gives a positive solution to (3.6). □

Theorem 3. *If (a, b) is the positive solution of* (3.6) *for which $x + y\sqrt{d}$ is minimized, then the equation has just the solutions $(\pm a_n, \pm b_n)$ given by* (3.8)*, where $n \in \omega$.*

Proof. Let (a, b), which exists by Lemma 2, be as in the statement. Then $a + b\sqrt{d} > 1$, so the powers of $a + b\sqrt{d}$ grow arbitrarily large. We know that all of the (a_n, b_n) are solutions of (3.6). Let (s, t) be an arbitrary positive solution. Then

$$(a + b\sqrt{d})^n \leqslant s + t\sqrt{d} < (a + b\sqrt{d})^{n+1}$$

for some non-negative n. Since $(a + b\sqrt{d})(a - b\sqrt{d}) = 1$, and $a+b\sqrt{d}$ is positive, so is $a-b\sqrt{d}$. Therefore, when we multiply by the nth power of this, we get

$$1 \leqslant (s + t\sqrt{d})(a - b\sqrt{d})^n < a + b\sqrt{d}. \tag{3.10}$$

But we have

$$(s \pm t\sqrt{d})(a \mp b\sqrt{d})^n = \ell \pm m\sqrt{d}$$

for some integers ℓ and m. This makes (ℓ, m) a solution of (3.6), and from (3.10) we now have

$$(\ell + m\sqrt{d})(\ell - m\sqrt{d}) \leqslant \ell + m\sqrt{d} < a + b\sqrt{d},$$
$$0 < \ell - m\sqrt{d} \leqslant 1 \leqslant \ell + m\sqrt{d},$$

so $m \geqslant 0$, and therefore $\ell > 0$. By minimality of $a + b\sqrt{d}$, we must have $\ell + m\sqrt{d} = 1$, so $(s, t) = (a_n, b_n)$. □

4. March 4, 2008 (Tuesday)

Quadratic fields

Every field L is a vector space over its every subfield F, and the dimension is denoted by

$$[L : F].$$

A subfield K of $\mathbb{C}$ such that $[K : \mathbb{Q}] = 2$ is called a **quadratic field.** Henceforth

$$\boxed{\text{let } K \text{ be a quadratic field.}}$$

The letter stands for the German *Körper* "body," this being the name, in languages other than English and Russian, for a field. Thus Russian поле, but French *corps* and Turkish *cisim.*

An integer that is indivisible by the square of any prime is called **square-free.** Thus 1, 2, and 3 are square-free, but 0, 4, and 12 are not. We may recall that the Möbius function of a square-free positive integer n is -1 raised to the power of the number of prime factors of n; if n is not square-free, then $\mu(n) = 0$.

For any α in $\mathbb{C}$, we let

$$\mathbb{Q}(\alpha)$$

denote the smallest subfield of $\mathbb{C}$ that contains α, while

$$\mathbb{Z}[\alpha]$$

is the smallest sub-*ring* of $\mathbb{C}$ that contains α. It is easy to see that this ring is $\{x + \alpha y \colon (x, y) \in \mathbb{Z} \times \mathbb{Z}\}$. It is not so easy to say what $\mathbb{Q}(\alpha)$ is; but we are interested only in the quadratice case.

Theorem 4. *The quadratic fields are just the fields $\mathbb{Q}(\sqrt{d})$, where d is a square-free integer, possibly negative, different from* 1.

Proof. Every K as above must contain some irrational x. Then 1 and x are linearly independent over $\mathbb{Q}$, so $\{1, x\}$ must be a basis over $\mathbb{Q}$ of K as a vector space. In particular, x^2 is a rational linear combination of 1 and x, which means

$$x^2 + bx + c = 0 \tag{4.1}$$

for some b and c in $\mathbb{Q}$. Thus

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

We can write $b^2 - 4c$ as $s^2 d$, where $s \in \mathbb{Q}$ and d is as described. Then $\sqrt{d} \in K \smallsetminus \mathbb{Q}$, so $\{1, \sqrt{d}\}$ is a basis of K. This means, as a space, K is

$$\mathbb{Q} \oplus \mathbb{Q}\sqrt{d}.$$

Every subfield of $\mathbb{C}$ containing $\sqrt{d}$ must include this space. This space must therefore be $\mathbb{Q}(\sqrt{d})$. It is an exercise to check that, conversely, for any d as described, the two-dimensional space $\mathbb{Q} \oplus \mathbb{Q}\sqrt{d}$ is indeed the field $\mathbb{Q}(\sqrt{d})$. In particular, if $a, b \in \mathbb{Q}$, and $b \neq 0$, then

$$\frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - b^2 d} = \frac{a}{a^2 - b^2 d} - \frac{b}{a^2 - b^2 d}\sqrt{d}.$$

Thus non-zero elements of $\mathbb{Q} \oplus \mathbb{Q}\sqrt{d}$ have multiplicative inverses. □

A rational number is an integer if and only if it satisfies an equation

$$x + c = 0,$$

where $c \in \mathbb{Z}$. This is a trivial observation, but it motivates the following definition. An element of K is an **integer** of K if it is an integer in the old sense, or else it satisfies an equation (4.1), where now b and c are in $\mathbb{Z}$. Henceforth, integers in the old sense can be called **rational integers.** More generally, the **algebraic integers** are the complex numbers that are roots of equations

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0,$$

where $a_i \in \mathbb{Z}$ and n ranges over the positive rational integers; but we shall not go beyond the quadratic case, $n = 2$.

Gaussian integers

For our first specific example of a quadratic field, we shall use the standard abbreviation

$$\mathrm{i} = \sqrt{-1}.$$

The integers of $\mathbb{Q}(\mathrm{i})$ are called the **Gaussian integers.**

The following is a special case of what we shall prove as Theorem 11.

Theorem 5. *The Gaussian integers compose the ring* $\mathbb{Z}[\mathrm{i}]$.

Proof. Let α be $m+n\,\mathrm{i}$ in $\mathbb{Z}[\mathrm{i}]$. Then $(\alpha - m)^2 = (n\,\mathrm{i})^2 = -n^2$, so $\alpha^2 - 2m\alpha + m^2 + n^2 = 0$, and thus α is a Gaussian integer.

Suppose conversely α is a Gaussian integer. By definition, $\alpha^2 + b\alpha + c = 0$ for some b and c in $\mathbb{Z}$. Hence

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Since $\alpha \in \mathbb{Q}(\,\mathrm{i}\,)$, the absolute value $|b^2 - 4c|$ must be a square in $\mathbb{Z}$. Say this square is e^2. Now α is one of

$$\frac{-b \pm e}{2}, \qquad\qquad \frac{-b \pm e\,\mathrm{i}}{2}.$$

Since $b^2 - 4c = \pm e^2$, we have

$$b^2 \mp e^2 \equiv 4c \equiv 0 \pmod 4, \qquad b \equiv e \pmod 2.$$

If b and e are both even, then α is in $\mathbb{Z}$ or $\mathbb{Z} \oplus \mathbb{Z}\,\mathrm{i}$; if odd, then $4 \nmid b^2 + e^2$, so it must be that $b^2 - e^2 = 4c$, which means $b^2 - 4c = e^2$, so that $\alpha \in \mathbb{Z}$. □

The **norm** on $\mathbb{Q}(\,\mathrm{i}\,)$ is the function given by

$$\begin{aligned} \mathrm{N}\,(a + b\,\mathrm{i}\,) &= a^2 + b^2 \\ &= |a + b\,\mathrm{i}\,|^2. \end{aligned} \tag{4.2}$$

The values are non-negative rational numbers, and

$$\mathrm{N}\,(\alpha\beta) = \mathrm{N}\,(\alpha)\,\mathrm{N}\,(\beta)\,.$$

Since

$$\frac{1}{a + b\,\mathrm{i}} = \frac{a - b\,\mathrm{i}}{a^2 + b^2} = \frac{a - b\,\mathrm{i}}{\mathrm{N}\,(a + b\,\mathrm{i}\,)},$$

we have

$$\frac{1}{a + b\,\mathrm{i}} \in \mathbb{Z}[\,\mathrm{i}\,] \iff \mathrm{N}\,(a + b\,\mathrm{i}\,) = \pm 1 \iff \mathrm{N}\,(a + b\,\mathrm{i}\,) = 1.$$

In short, $a + b\,\mathrm{i}$ is a unit of $\mathbb{Z}[\,\mathrm{i}\,]$ if and only if $a^2 + b^2 = 1$. In particular, the unit Gaussian integers are ± 1 and $\pm\,\mathrm{i}$.

5. March 7, 2008 (Friday)

Euclidean domains

An **integral domain** (*tamlık alanı*), or simply a **domain,** is a sub-ring of a field. For us, the field will usually be $\mathbb{C}$. As an example, $\mathbb{Z}[\,\mathrm{i}\,]$ is an integral domain. A *Euclidean domain* is a domain in which the Euclidean algorithm works. This means two things:

1) we can perform division with remainder, where the remainder is "smaller" than the divisor;
2) a sequence of remainders of decreasing size must terminate.

Since decreasing sequences of natural numbers must terminate, we shall use natural numbers to measure size. Formally, a domain R is a **Euclidean domain** if there is a function $x \mapsto \mathrm{d}(x)$, the **degree,** from $R \setminus \{0\}$ into ω such that, for all α and β in R, if $\beta \neq 0$, then the system

$$\alpha = \beta x + y \;\;\&\;\; \mathrm{d}(y) < \mathrm{d}(\beta)$$

is soluble in R.

Gaussian integers have a size, namely their absolute value, but this need not be a rational integer. Since the *square* is one, we let $\mathrm{d}(x)$ be the norm $\mathrm{N}\,(x)$ as in (4.2).

Theorem 6. $\mathbb{Z}[\,\mathrm{i}\,]$, *as equipped with the norm, is a Euclidean domain.*

Proof. Given α and β in $\mathbb{Z}[\,\mathrm{i}\,]$, where $\beta \neq 0$, we must solve

$$\alpha = \beta x + y \;\;\&\;\; \mathrm{N}\,(y) < \mathrm{N}\,(\beta)$$

The Gaussian-integral multiples of β compose a square **lattice** (*kafes*) in $\mathbb{C}$, as in Figure 5.1. Then α is in one of the squares

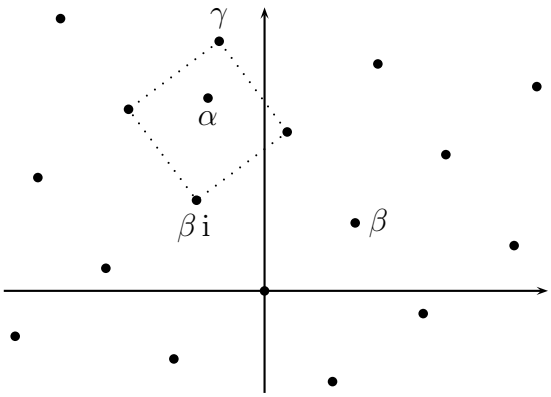

Figure 5.1.: A lattice of Gaussian multiples

whose vertices are among these multiples. The closest vertex to α is some γ such that

$$|\alpha - \gamma| \leqslant \frac{\sqrt{2}}{2}|\beta|, \qquad \mathrm{N}\,(\alpha - \gamma) \leqslant \frac{1}{2}\,\mathrm{N}\,(\beta)\,.$$

So our solution is $(\gamma/\beta, \alpha - \gamma)$. □

Doing the proof more algebraically, we have $\alpha/\beta = r + s\,\mathrm{i}$ for some r and s in $\mathbb{Q}$. There are m and n in $\mathbb{Z}$ such that $|r - m|, |s - n| \leqslant 1/2$. Then

$$\begin{aligned}\mathrm{N}\,(\alpha - \beta(m + n\,\mathrm{i}\,)) &= \mathrm{N}\,(\beta)\,\mathrm{N}\left(\frac{\alpha}{\beta} - (m + n\,\mathrm{i}\,)\right) \\ &= \mathrm{N}\,(\beta)\,\mathrm{N}\,(r - m + (s - n)\,\mathrm{i}\,) \leqslant \frac{1}{2}\,\mathrm{N}\,(\beta)\,.\end{aligned}$$

Now we can find *greatest common divisors* in $\mathbb{Z}[\,\mathrm{i}\,]$. In any domain, a **greatest common divisor** of two elements α and β, not both 0, is a common divisor that is divisible by every other common divisor. This greatest common divisor need not be unique. Two greatest common divisors divide each other and so are called **associates.** Conversely, the associate of a greatest common divisor is a greatest common divisor.

Problem 4. *Find in* $\mathbb{Z}[\,\mathrm{i}\,]$ *a greatest common divisor of* $7+6\,\mathrm{i}$ *and* $-1+7\,\mathrm{i}$.

Solution. Following the pattern of the Euclidean Algorithm as on page 24, we compute first

$$\frac{7+6\,\mathrm{i}}{-1+7\,\mathrm{i}} = \frac{(7+6\,\mathrm{i})(-1-7\,\mathrm{i})}{50} = \frac{35-55\,\mathrm{i}}{50} = \frac{7-11\,\mathrm{i}}{10}$$
$$= \frac{10-3-(10+1)\,\mathrm{i}}{10} = 1-\,\mathrm{i}\,+\frac{-3-\,\mathrm{i}}{10},$$

and then

$$\frac{(-1+7\,\mathrm{i})(-3-\,\mathrm{i}\,)}{10} = 1-2\,\mathrm{i}\,,$$

so that, finally

$$\frac{-1+7\,\mathrm{i}}{1-2\,\mathrm{i}} = \frac{10}{-3-\,\mathrm{i}} = -3+\,\mathrm{i}\,.$$

Thus, in sum,

$$\begin{aligned} 7+6\,\mathrm{i} &= (-1+7\,\mathrm{i})(1-\,\mathrm{i}\,)+1-2\,\mathrm{i}\,, \\ -1+7\,\mathrm{i} &= (1-2\,\mathrm{i}\,)(-3+\,\mathrm{i}\,). \end{aligned}$$

In particular, $1-2\,\mathrm{i}$ is a greatest common divisor of $7+6\,\mathrm{i}$ and $-1+7\,\mathrm{i}$. The other greatest common divisors are obtained by multiplying by the units of $\mathbb{Z}[\,\mathrm{i}\,]$, namely ±1 and $\pm\,\mathrm{i}$. So they are $\pm(1-2\,\mathrm{i}\,)$ and $\pm(2+\,\mathrm{i}\,)$. □

6. March 11, 2008 (Tuesday)

Unique-factorization domains

All Euclidean domains are *principal-ideal domains*, and all principal-ideal domains are **unique-factorization domains.** Therefore $\mathbb{Z}[\,\mathrm{i}\,]$ is a unique-factorization domain; but we can also prove this directly, using that

$$\mathrm{N}\,(\xi\eta) = \mathrm{N}\,(\xi)\,\mathrm{N}\,(\eta)\,.$$

First, an element of any domain, other than 0 or a unit, is **irreducible** if its only divisors are itself and units. Suppose α is a reducible Gaussian integer. Then

$$\alpha = \beta\gamma$$

for some β and γ, neither of which is a unit. But then $\mathrm{N}\,(\beta)$ and $\mathrm{N}\,(\gamma)$ are greater than 1, so

$$1 < \mathrm{N}\,(\beta) < \mathrm{N}\,(\alpha)\,, \qquad 1 < \mathrm{N}\,(\gamma) < \mathrm{N}\,(\alpha)\,.$$

Since there is no infinite strictly decreasing sequence of natural numbers, the process of factorizing the factors of α as products of non-units must terminate. Thus α can be written as a product of irreducible factors.

The definition of unique-factorization domain requires that irreducible factorizations must be unique. This means, if

$$\alpha_0\alpha_1\cdots\alpha_m = \beta_0\beta_1\cdots\beta_n,$$

where each α_i and each β_j are irreducible, then each α_i must be an associate of some β_j. To prove this for $\mathbb{Z}[\,\mathrm{i}\,]$, it is enough to show that each irreducible Gaussian integer is *prime.* In any domain, an element α (not 0 or a unit) is **prime,** provided

$$\alpha \mid \beta\gamma \;\;\&\;\; \alpha \nmid \beta \implies \alpha \mid \gamma.$$

In $\mathbb{Z}[\,\mathrm{i}\,]$, suppose α is irreducible, and $\alpha \mid \beta\gamma \;\;\&\;\; \alpha \nmid \beta$. Then the greatest common divisors of α and β are just the units. By applying the Euclidean Algorithm, we can solve the equation

$$\alpha\xi + \beta\eta = 1$$

$\mathbb{Z}[\,\mathrm{i}\,]$. But then

$$\alpha\gamma\xi + \beta\gamma\eta = \gamma,$$

and since α divides the summands on the left, it divides γ.

Gaussian primes

We now ask: What are the primes of $\mathbb{Z}[\,\mathrm{i}\,]$? Suppose π is one of them. Then π is not a unit, so $\mathrm{N}\,(\pi)$ has rational-prime factors. But

$$\pi\overline{\pi} = \mathrm{N}\,(\pi)\,.$$

Therefore, since π is prime, we have

$$\pi \mid p$$

for some rational-prime factor of $\mathrm{N}\,(\pi)$. If q is another rational prime, then $ap + bq = 1$ for some rational integers a and b. Since $\pi \nmid 1$, it must be that $\pi \nmid q$. Thus p is unique.

Theorem 7. *The Gaussian primes are just the associates of the following:*

(i) $1 + \mathrm{i}$;
(ii) *the rational primes* p, *where* $p \equiv 3 \pmod 4$;
(iii) α, *where* $\mathrm{N}(\alpha)$ *is a rational prime* p *such that* $p \equiv 1 \pmod 4$ *(and two such non-associated* α *exist for every such* p*).*

Proof. We have just seen that every Gaussian prime π divides some rational prime p. Then $\mathrm{N}(\pi)$ divides $\mathrm{N}(p)$, which is p^2; so $\mathrm{N}(\pi)$, which is $\pi\overline{\pi}$, is either p or p^2. Also $\mathrm{N}(\pi)$ is of the form $x^2 + y^2$, so it is congruent to 0, 1, or 2, *modulo* 4.

Suppose now $p \equiv 3 \pmod 4$. Then we must have

$$\pi\overline{\pi} = p^2.$$

But $\pi\overline{\pi}$ is a prime factorization, so it is unique as such. Therefore π and $\overline{\pi}$ are associates of p and hence of each other. In short, p is a Gaussian prime.

In case $p = 2$, we note

$$2 = (1 + \mathrm{i})(1 - \mathrm{i}).$$

Also, $1 \pm \mathrm{i}$ must be irreducible, since $\mathrm{N}(1 \pm \mathrm{i}) = 2$ (so if $1 \pm \mathrm{i} = \alpha\beta$, then α or β must have norm 1 and so be a unit). So we have the unique prime factorization of 2. Also $1 + \mathrm{i}$ and $1 - \mathrm{i}$ are associates. Hence the only prime divisors of 2 are the four associates

$$1 + \mathrm{i}, \quad 1 - \mathrm{i}, \quad -1 + \mathrm{i}, \quad -1 - \mathrm{i}.$$

Finally, suppose $p \equiv 1 \pmod 4$. Then -1 is a quadratic residue *modulo* p, so $-1 \equiv x^2 \pmod p$ for some x, that is, $p \mid 1 + x^2$, and therefore

$$p \mid (1 + x\,\mathrm{i})(1 - x\,\mathrm{i}).$$

But $(1 \pm x\,\mathrm{i}\,)/p$ is *not* a Gaussian integer. Therefore p must not be a Gaussian prime. Consequently, if π is a prime factor of p, then $\mathrm{N}\,(\pi) = p$, that is,

$$\pi\overline{\pi} = p.$$

This is a prime factorization. Moreover, π and $\overline{\pi}$ are not associates. Indeed, $\pi = x + y\,\mathrm{i}$ for some rational integers x and y, so that

$$\frac{\pi}{\overline{\pi}} = \frac{(x + y\,\mathrm{i}\,)^2}{p} = \frac{x^2 - y^2 + 2xy\,\mathrm{i}}{p}.$$

If this is a Gaussian integer, then $p \mid 2xy$, so $p \mid xy$ (since p is odd), so $p < x^2 + y^2 = p$, which is absurd. □

If n is a positive rational integer, then the Diophantine equation (1.4) of Problem 3, namely $x^2 + y^2 = n$, is soluble if and only if the equation

$$\mathrm{N}\,(\xi) = n \tag{6.1}$$

is soluble, where ξ is a Gaussian integer. Moreover, there is a bijection $(x, y) \mapsto x + y\,\mathrm{i}$ between the solution-sets. This gives us an alternative solution to Problem 3:

Corollary. *In case n is a rational prime p, the equation* (1.4) *has a solution if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*

We can also *count* solutions. Suppose $p \equiv 1 \pmod 4$. If $n = p$, then (6.1) has exactly 8 solutions: the associates of π for some prime π, and the associates of $\overline{\pi}$. If $n = p^2$, the solutions are the associates of π^2, of $\pi\overline{\pi}$, and of $\overline{\pi}^2$, so there are 12 solutions. If q is another prime, but still $q \equiv 1 \pmod 4$, and $n = pq$, then there are 16 solutions. In this way we obtain the following; details are an exercise.

Theorem 8. *The number of solutions of* (1.4) *is* $4(a-b)$, *where*

$$\begin{aligned} a &= |\{x \in \omega \colon x \mid n \ \ \& \ \ x \equiv 1\}| \\ b &= |\{x \in \omega \colon x \mid n \ \ \& \ \ x \equiv 3\}| \end{aligned} \pmod 4.$$

Theorem 9. *Letting* π *be (as usual) the circumference of the unit circle, we have*

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots$$

Proof. The area of a circle of radius r is πr^2. Hence

$$\pi r^2 \approx |\{\xi \in \mathbb{Z}[\,\mathrm{i}\,] \colon 1 \leqslant |\xi| \leqslant r\}| = \sum_{n=1}^{r^2} |\{\xi \in \mathbb{Z}[\,\mathrm{i}\,] \colon \mathrm{N}\,(\xi) = n\}|.$$

(See Figure 6.1.) By Theorem 8, to this number, each positive

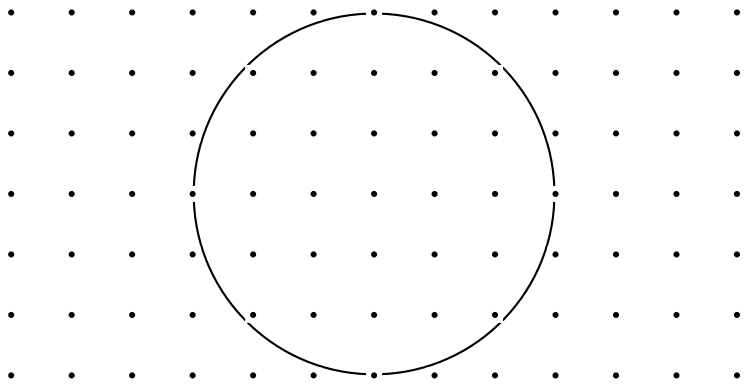

Figure 6.1.: Estimating the area of a circle

$4m+1$ contributes 4 for each of its multiples between 1 and r^2,

while each positive $4m+3$ takes away 4 for each such multiple. Therefore

$$\frac{\pi r^2}{4} \approx \sum_{n=0}^{\infty} \left(\left[\frac{r^2}{4n+1} \right] - \left[\frac{r^2}{4n+3} \right] \right)$$
$$= r^2 - \left[\frac{r^2}{3} \right] + \left[\frac{r^2}{5} \right] - \left[\frac{r^2}{7} \right] + \cdots$$

Dividing by r^2 and taking the limit yields the claim. (For details, see [7, pp. 32–9].) □

Arbitrary quadratic fields

Recall the Pell equation (3.6) on page 29, which we can factorize as

$$1 = (x + y\sqrt{d})(x - \sqrt{d}). \tag{6.2}$$

This suggests looking at $\mathbb{Q}(\sqrt{d})$. We eliminated some trivial cases before, and one of them was $d < 0$. Now we shall allow this, but shall henceforth require

that d be a square-free integer other than 1.

Let us also henceforth suppose

$$K = \mathbb{Q}(\sqrt{d}).$$

On K we define $\xi \mapsto \xi'$ by

$$(a + b\sqrt{d})' = a - b\sqrt{d}. \tag{6.3}$$

When $d < 0$, this is complex conjugation. In any case, we define the **trace** and **norm** of α by

$$\mathrm{Tr}(\alpha) = \alpha + \alpha', \qquad \mathrm{N}(\alpha) = \alpha\alpha' \tag{6.4}$$

respectively. These are rational numbers. Indeed, if $\alpha = a + b\sqrt{d}$, then

$$\mathrm{Tr}(\alpha) = 2a, \qquad \mathrm{N}(\alpha) = a^2 - b^2 d.$$

Theorem 10. *An element of K is an integer if and only if its norm and trace are rational integers.*

Proof. Let $\alpha \in K$. Since

$$(x - \alpha)(x - \alpha') = x^2 - (\alpha + \alpha')x + \alpha\alpha',$$

α is a zero of the polynomial

$$x^2 - \mathrm{Tr}(\alpha)x + \mathrm{N}(\alpha). \tag{6.5}$$

Thus if the trace and norm of α are rational integers, then α is an integer, by the definition on page 35. Conversely, if α is an integer, then either α is a rational integer, or else the polynomial in (6.5) must be the **minimal polynomial** of α over $\mathbb{Q}$, that is, the polynomial of least degree with rational coefficients, and leading coefficient 1, of which α is a root. (This must exist, since the ring $\mathbb{Q}[x]$ of polynomials is a Euclidean domain with respect to polynomial degree.) In either case, the norm and trace of α must be rational integers. □

The set of integers of K can be denoted by

$$\mathfrak{O}_K.$$

As in case $d = -1$ with Theorem 5, so generally, we want to show that $\mathfrak{O}_K$ is a sub-ring of K, thus an integral domain. This means showing $\mathfrak{O}_K$ contains 0 and 1 and is closed under

addition, subtraction, and multiplication. Obviously $\mathfrak{O}_K$ contains 0 and 1, since it includes $\mathbb{Q}$. If α satisfies (4.1) on page 34, then $-\alpha$ satisfies

$$x^2 - bx + c = 0;$$

thus $\mathfrak{O}_K$ is closed under additive inversion. It remains to show $\mathfrak{O}_K$ is closed under addition and multiplication. For this, by Lemma 10, assuming the norms and traces of α and β are in $\mathbb{Z}$, we need only show that so are the norms and traces of $\alpha+\beta$ and $\alpha\beta$. Since $(\alpha+\beta)' = \alpha' + \beta'$ and $(\alpha\beta)' = \alpha'\beta'$, we have

$$\mathrm{Tr}(\alpha+\beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta), \qquad \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta).$$

Since $(\alpha+\beta)(\alpha'+\beta') = \alpha\alpha' + \alpha\beta' + \alpha'\beta + \beta\beta'$, we have

$$\mathrm{N}(\alpha+\beta) = \mathrm{N}(\alpha) + \mathrm{Tr}(\alpha\beta') + \mathrm{N}(\beta).$$

Thus it is enough to show $\mathrm{Tr}(\alpha\beta') \in \mathbb{Z}$. Letting

$$\alpha = a_0 + a_1\sqrt{d}, \qquad \beta = b_0 + b_1\sqrt{d},$$

so that $\alpha\beta' = a_0b_0 - a_1b_1d - (a_0b_1 - a_1b_0)\sqrt{d}$, we are assuming $\mathbb{Z}$ contains all of

$$2a_0, \qquad 2b_0, \qquad {a_0}^2 - {a_1}^2 d, \qquad {b_0}^2 - {b_1}^2 d,$$

and we have to show $\mathbb{Z}$ also contains $a_0b_0 - a_1b_1d$. This is left as an exercise, which can be solved independently or by Theorem 11 below.

7. March 14, 2008 (Friday)

As on page 34,

$$\mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d} = \{x + y\sqrt{d} \colon (x, y) \in \mathbb{Z} \times \mathbb{Z}\}.$$

It follows now that $\mathbb{Z}[\sqrt{d}] \subseteq \mathfrak{O}_K$. The converse fails when $d \equiv 1 \pmod 4$, since $(1 + \sqrt{d})/2$ has the minimal polynomial $x^2 - x + (1 - d)/4$. In order to characterize $\mathfrak{O}_K$, we define

$$\omega = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2 \text{ or } 3 \pmod 4; \\ \dfrac{1 + \sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod 4. \end{cases} \tag{7.1}$$

Henceforth ω shall always have this meaning.

Note that, in any case of d, we have $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Z}[\omega]$.

Theorem 11. $\mathfrak{O}_K = \mathbb{Z}[\omega]$.

Proof. Let α be an element $a + b\sqrt{d}$ of K, so that α is a zero of the polynomial

$$x^2 - 2ax + a^2 - b^2 d. \tag{7.2}$$

Suppose first $\alpha \in \mathfrak{O}_K$. Then $2a$ and $a^2 - b^2 d$ are in $\mathbb{Z}$ by Lemma 10. There are two cases.

(i) If $2a$ is even, then $a \in \mathbb{Z}$, so $b^2 d \in \mathbb{Z}$, and hence $b \in \mathbb{Z}$ since d is square-free; consequently $\alpha \in \mathbb{Z}[\sqrt{d}]$, and so $\alpha \in \mathbb{Z}[\omega]$.

(ii) Suppose $2a$ is odd. *Modulo* 4 we have $4a^2 \equiv (2a)^2 \equiv 1$. But also $4a^2 - 4b^2 d \equiv 0$, so that $(2b)^2 d \equiv 4b^2 d \equiv 4a^2 \equiv 1$. Since $2b \in \mathbb{Z}$, again because d is square-free, we have $(2b)^2$ congruent to 0 or 1, and therefore $(2b)^2 \equiv 1$. We conclude both that $2b$ is odd and that $d \equiv 1$. Again we obtain $\alpha \in \mathbb{Z}[\omega]$.

Suppose conversely $\alpha \in \mathbb{Z}[\omega]$. *Modulo* 4, if d is not congruent to 1, then a and b are rational integers, so the polynomial in (7.2) is over $\mathbb{Z}$, and thus $\alpha \in \mathfrak{O}_K$. If d *is* congruent to 1, then both $2a$ and $2b$ must be integers, and moreover $2a \equiv 2b \pmod 2$, so that

$$4(a^2 - b^2 d) \equiv (2a)^2 - (2b)^2 \equiv 0 \pmod 4,$$

and again the polynomial in (7.2) is over $\mathbb{Z}$. □

Quadratic forms

Assuming $a, b, c \in \mathbb{Q}$, let

$$f(x, y) = ax^2 + bxy + cy^2; \tag{7.3}$$

this is a **binary quadratic form.** We shall investigate the rational-integral solutions of

$$f(x, y) = m,$$

where $m \in \mathbb{Q}$. The Pell equation (3.6), rewritten as (6.2), is a special case. Assuming $a \neq 0$, we can factorize f over an

appropriate quadratic field by completing the square:

$$\begin{aligned} f(x,y) &= a\Big(x^2 + \frac{b}{a}\cdot xy + \frac{b^2}{4a^2}\cdot y^2\Big) - \Big(\frac{b^2}{4a} - c\Big)y^2 \\ &= a\Big(x + \frac{b}{2a}\cdot y\Big)^2 - \Big(\frac{b^2}{4a} - c\Big)y^2 \\ &= \frac{1}{a}\Big(ax + \frac{b}{2}\cdot y\Big)^2 - \frac{1}{a}\Big(\frac{b^2}{4} - ac\Big)y^2. \end{aligned}$$

Letting $D = b^2 - 4ac$, the **discriminant** of f, we have

$$\begin{aligned} f(x,y) &= \frac{1}{a}\left[\Big(ax + \frac{b}{2}\cdot y\Big)^2 - \frac{D}{4}\cdot y^2\right] \\ &= \frac{1}{a}\Big(ax + \frac{b}{2}\cdot y + \frac{\sqrt{D}}{2}\cdot y\Big)\Big(ax + \frac{b}{2}\cdot y - \frac{\sqrt{D}}{2}\cdot y\Big) \\ &= \frac{1}{a}\Big(ax + \frac{b+\sqrt{D}}{2}\cdot y\Big)\Big(ax + \frac{b-\sqrt{D}}{2}\cdot y\Big). \end{aligned}$$

Assuming $\sqrt{D}$ is irrational, we can write D as $s^2 d$, where s is a nonzero rational number, while d is a square-free rational integer different from 1, as per the convention established on page 45. working in K, which is by our convention $\mathbb{Q}(\sqrt{d})$, and letting

$$\alpha = a, \qquad \beta = \frac{b+\sqrt{D}}{2} = \frac{b+s\sqrt{d}}{2},$$

we have

$$f(x,y) = \frac{1}{a}(\alpha x + \beta y)(\alpha' x + \beta' y) = \frac{1}{a}\,\mathrm{N}\,(\alpha x + \beta y)\,.$$

Moreover, α and β are linearly independent over $\mathbb{Q}$; that is, the only rational solution to $\alpha x + \beta y = 0$ is $(0,0)$.

For any α and β in K, we may denote the set $\{\alpha x + \beta y : x, y \in \mathbb{Z}\}$ of all rational-integral linear combinations of α and β by either of

$$\mathbb{Z}\alpha + \mathbb{Z}\beta, \qquad\qquad \langle \alpha, \beta \rangle.$$

If α and β are linearly independent over $\mathbb{Q}$, then $\langle \alpha, \beta \rangle$ is a **lattice** in K, to be denoted by Λ. This means two things:

(i) Λ is a *free abelian subgroup* of K;

(ii) the minimum number of generators of this group is the dimension $[K : \mathbb{Q}]$.

In short,

$$\boxed{\Lambda \text{ is } \mathbb{Z}\alpha \oplus \mathbb{Z}\beta.}$$

For example, by Theorem 11, as a group, $\mathfrak{O}_K$ is the lattice $\langle 1, \omega \rangle$. In general, if Λ is a lattice in K, let

$$\mathrm{End}(\Lambda) = \{\xi \in \mathbb{C} \colon \xi\Lambda \subseteq \Lambda\}.$$

This set is a sub-ring of K and and can be understood as the ring of **endomorphisms** of the abelian group Λ. That is, the function $\xi \mapsto \alpha\xi$ is an endomorphism of Λ if and only if $\alpha \in \mathrm{End}(\Lambda)$.

For example, if $\Lambda = \langle 1, \mathrm{i} \rangle$, then $\mathrm{End}(\Lambda) = \langle 1, \mathrm{i} \rangle$. But suppose $\Lambda = \langle 1, \tau \rangle$, where

$$\tau = \frac{-1 + \sqrt{-7}}{4}. \tag{7·4}$$

Then $(4\tau + 1)^2 = -7$, so $16\tau^2 + 8\tau + 8 = 0$, which means $2\tau^2 + \tau + 1 = 0$, that is, $2\tau^2 = -\tau - 1$, and therefore

$$2\tau\Lambda = \langle 2\tau, -\tau - 1 \rangle = \langle 2, \tau + 1 \rangle.$$

See Figure 7.1. In particular, $\langle 1, 2\tau \rangle \subseteq \mathrm{End}(\Lambda)$. Conversely, if $x + y\tau \in \mathrm{End}(\Lambda)$, then Λ contains $(x + y\tau)\tau$, but

$$(x + y\tau)\tau = x\tau + y\tau^2 = x\tau + y\frac{-\tau - 1}{2} = -\frac{y}{2} + \Big(x - \frac{y}{2}\Big)\tau,$$

So y must be even. Thus $\mathrm{End}(\Lambda) = \langle 1, 2\tau \rangle$.

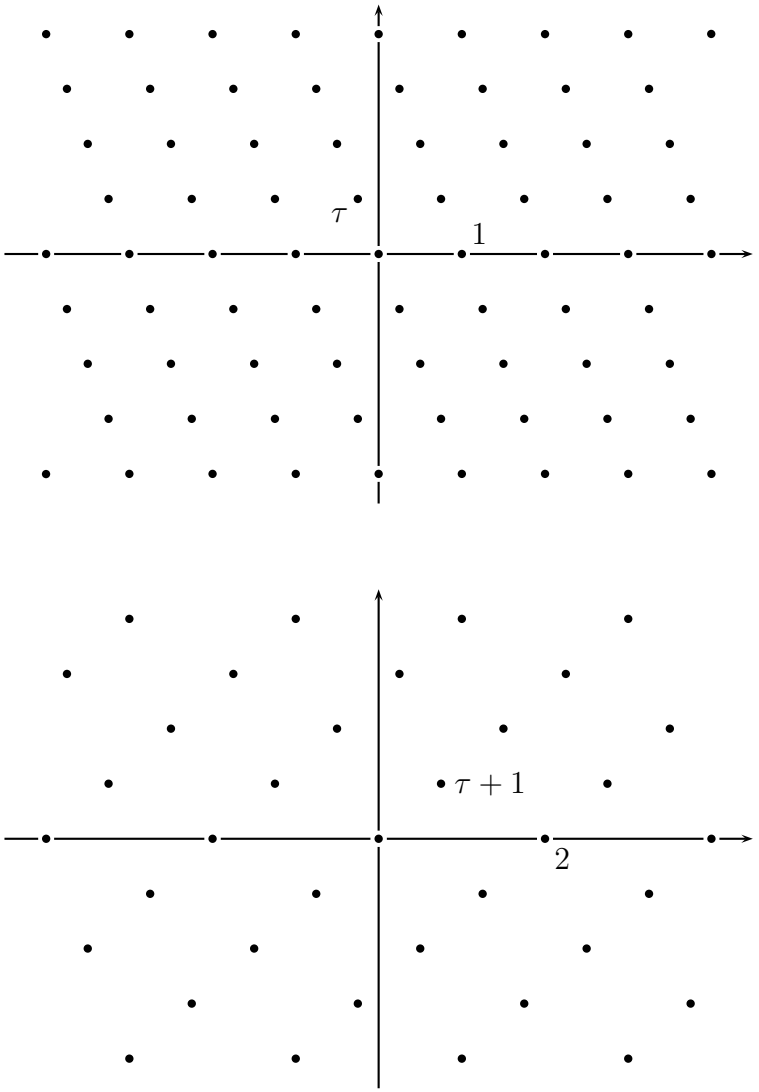

Figure 7.1.: Lattice and isomorphic sublattice, τ as in (7.4)

8. March 18, 2008 (Tuesday)

Lattices and elliptic curves

To get a sense for where things may lead (not in this course, but see for example [9]), suppose Λ is a lattice, merely in the sense that $\alpha \neq 0$ and $\beta/\alpha \notin \mathbb{R}$; the complex numbers α and β need not be quadratic. Geometrically, the quotient group $\mathbb{C}/\Lambda$ is the parallelogram shown in Figure 8.1, but opposite edges

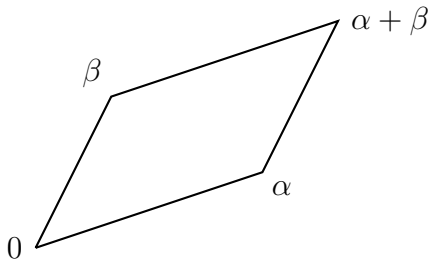

Figure 8.1.: A fundamental parallelogram of a lattice

are identified; thus the quotient is a **torus.** The holomorphic function $\wp$ called the **Weierstraß functioni**s given by

$$\wp(z) = \frac{1}{z^2} + \sum_{\zeta \in \Lambda \smallsetminus \{0\}} \Big(\frac{1}{(z-\zeta)^2} - \frac{1}{\zeta^2} \Big)$$

and is **doubly periodic,** with period Λ, meaning

$$\zeta \in \Lambda \iff \wp(z+\zeta) = \wp(z) \text{ for all } z.$$

Hence $\wp$ is well-defined as a function on the torus $\mathbb{C}/\Lambda$. There are complex numbers g_2 and g_3, depending on Λ, such that $(\wp(z), \wp'(z))$ solves the equation

$$y^2 = 4x^3 - g_2 x - g_3.$$

This equation defines an **elliptic curve,** such as in Figure 8.2. This curve is an abelian group by the rule that $P + Q + R = 0$

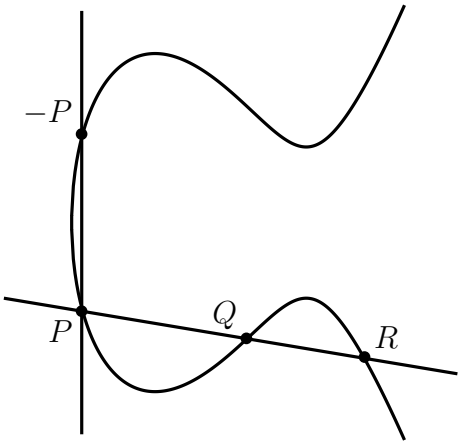

Figure 8.2.: An elliptic curve

when the three points are collinear. Here 0 is the point at infinity, met by every vertical line. Then $(\wp, \wp')$ is an isomorphism from $\mathbb{C}/\Lambda$ to the elliptic curve.

An analytic endomorphism of $\mathbb{C}/\Lambda$ is a function $z \mapsto \gamma z$, where $\gamma \in \mathbb{C}$, such that $\gamma\Lambda \subseteq \Lambda$. The set of these α is what we are calling $\mathrm{End}(\Lambda)$. Always $\mathbb{Z} \subseteq \mathrm{End}(\Lambda)$. You can show that $\mathbb{Z} = \mathrm{End}(\Lambda)$ if and only if β/α is not quadratic.

Quadratic lattices

We are interested in the quadratic case, and henceforth we assume

$$\boxed{\alpha \text{ and } \beta \text{ are in } K \text{ for some } d.}$$

Every element $\alpha x + \beta y$ of Λ is the matrix product

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Then $\langle \gamma, \delta \rangle \subseteq \langle \alpha, \beta \rangle$ if and only if the equation

$$\begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

is soluble in $\mathbb{Z}$. In particular, $\langle \gamma, \delta \rangle = \langle \alpha, \beta \rangle$ if and only if

$$\begin{pmatrix} \gamma \\ \delta \end{pmatrix} = M \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

for some *invertible* matrix M over $\mathbb{Z}$: this means $\det M = \pm 1$.

Along with the sub-ring $\mathrm{End}(\Lambda)$ of K, we have the sub-ring $\mathfrak{O}_K$. What is the relation between the two rings?

Lemma 3. $\mathrm{End}(\Lambda) \subseteq \mathfrak{O}_K$.

Proof. Suppose $\gamma \in \mathrm{End}(\Lambda)$. Then there are a, b, c, and d in $\mathbb{Z}$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \gamma \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \gamma & 0 \\ 0 & \gamma \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \gamma - a & -b \\ -c & \gamma - d \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Hence the last square matrix is not invertible over any field, so its determinant is 0. In particular, γ is a root of the equation

$$0 = (x-a)(z-d) - bc = x^2 - (a+d)x + ad - bc.$$

The coefficients belonging to $\mathbb{Z}$, we have $\gamma \in \mathfrak{O}_K$. □

Pell equation examples

Problem 5. *Solve the Pell equation*

$$x^2 - 14y^2 = 1. \tag{8.1}$$

Solution. We first find the continued fraction expansion of $\sqrt{14}$ by our algorithm:

$$\begin{aligned}
& & a_0 = 3, \quad & \xi_0 = \sqrt{14} - 3; \\
\frac{1}{\sqrt{14}-3} = \frac{\sqrt{14}+3}{5}, \quad & & a_1 = 1, \quad & \xi_1 = \frac{\sqrt{14}-2}{5}; \\
\frac{5}{\sqrt{14}-2} = \frac{\sqrt{14}+2}{2}, \quad & & a_2 = 2, \quad & \xi_2 = \frac{\sqrt{14}-2}{2}; \\
\frac{2}{\sqrt{14}-2} = \frac{\sqrt{14}+2}{5}, \quad & & a_3 = 1, \quad & \xi_3 = \frac{\sqrt{14}-3}{5}; \\
\frac{5}{\sqrt{14}-3} = \sqrt{14}+3, \quad & & a_4 = 6, \quad & \xi_4 = \sqrt{14} - 3 = \xi_0;
\end{aligned}$$

therefore

$$\sqrt{14} = [3; \overline{1, 2, 1, 6}]. \tag{8.2}$$

For the convergents p_n/q_n, we have

$$\frac{p_0}{q_0} = \frac{3}{1}, \qquad \frac{p_1}{q_1} = \frac{4}{1}, \qquad \frac{p_n}{q_n} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}$$

by (3.4), so the list is

$$\frac{3}{1}, \quad \frac{4}{1}, \quad \frac{11}{3}, \quad \frac{15}{4}, \quad \frac{101}{27}, \quad \dots$$

We check for a solution to (8.1):

$$\begin{aligned} 3^2 - 14 \cdot 1^2 &= -5, \\ 4^2 - 14 \cdot 1^2 &= 2, \\ 11^2 - 14 \cdot 3^2 &= 121 - 126 = -5, \\ 15^2 - 14 \cdot 4^2 &= 225 - (15-1)(15+1) = 1. \end{aligned}$$

Then $15/4 = [3; 1, 2, 1]$, and $(15, 4)$ solves (8.1). This is the positive solution (a, b) for which $a + b\sqrt{14}$ is least: we shall be able to conclude this from Theorem 26 on page 107, but meanwhile one can verify the claim by trying all pairs (a, b) such that $0 < a < 15$ and $0 < b < 4$. Then by Theorem 3 on page 31, every positive solution must be (a_n, b_n), where

$$a_n + b_n\sqrt{14} = (15 + 4\sqrt{14})^n.$$

Finally, $(a_n, b_n) = (p_{4n+3}, q_{4n+3})$. Indeed, if (k, ℓ) is a solution, then by the computation

$$(15 + 4\sqrt{14})(k + \ell\sqrt{14}) = 15k + 56\ell + (4k + 15\ell)\sqrt{14},$$

we have that $(15k + 56\ell, 4k + 15\ell)$ is a solution. But also,

writing (p_{4n+3}, q_{4n+3}) as (a, b), we have

$$\frac{p_{4n+7}}{q_{4n+7}} = \left[3; 1, 2, 1, 3 + \frac{a}{b}\right] = 3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{a}{b}}}}}$$

$$= 3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{b}{a + 3b}}}} = 3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{a + 3b}{a + 4b}}}$$

$$= 3 + \cfrac{1}{1 + \cfrac{a + 4b}{3a + 11b}} = 3 + \frac{3a + 11b}{4a + 15b} = \frac{15a + 56b}{4a + 15b}.$$

By induction, our claim is proved. □

The expansion $[3; \overline{1, 2, 1, 6}]$ of $\sqrt{14}$ has the period $(1, 2, 1, 6)$ of length 4, which is even. But

$$\sqrt{13} = [3; \overline{1, 1, 1, 1, 6}] \tag{8.3}$$

with a period of odd length 5. The convergents p_n/q_n of $\sqrt{d}$ are alternately above and below $\sqrt{d}$, this being irrational; in particular, the convergents p_{2n}/q_{2n} are below. Therefore $[3; 1, 1, 1, 1]$ cannot provide a solution to $x^2 - 13y^2 = 1$. But

$$[3; 1, 1, 1, 1, 6, 1, 1, 1, 1]$$

will provide the fundamental solution, which generates the others, so that the solutions here will be p_{10n+9}/q_{10n+9}. See page 99.

9. March 25, 2008 (Tuesday)

Quadratic form example

A problem on last night's examination was to find solutions to the Diophantine equation

$$2x^2 - 3y^2 = 2. \tag{9.1}$$

Let us define

$$\begin{aligned} f(x,y) = 2x^2 - 3y^2 &= 2\left(x^2 - \frac{3}{2}y^2\right) \\ &= 2\left(x + \sqrt{\frac{3}{2}} \cdot y\right)\left(x - \sqrt{\frac{3}{2}} \cdot y\right) \\ &= \frac{1}{2}(2x + \sqrt{6} \cdot y)(2x - \sqrt{6} \cdot y). \end{aligned}$$

Working in $\mathbb{Q}(\sqrt{6})$, we have

$$f(x,y) = \frac{1}{2}\,\mathrm{N}\left(2x + \sqrt{6} \cdot y\right) = \frac{1}{2}\,\mathrm{N}\left(\alpha x + \beta y\right),$$

where $\alpha = 2$ and $\beta = \sqrt{6}$. We have a bijection $(x,y) \mapsto \alpha x + \beta y$ between:

(i) the solution-set of (9.1);

(ii) the set of ξ in $\langle \alpha, \beta \rangle$ such that $\mathrm{N}(\xi) = 4$.

In particular, $(5,4)$ is a solution of (9.1), and $\mathrm{N}(5\alpha + 4\beta) = 4$. Then other solutions to $\mathrm{N}(\xi) = 4$ include $\varepsilon \cdot (5\alpha + 4\beta)$, provided:

(i) $\mathrm{N}(\varepsilon) = 1$;
(ii) $\varepsilon \cdot (5\alpha + 4\beta) \in \langle \alpha, \beta \rangle$,—and this is achieved if $\varepsilon\langle \alpha, \beta \rangle \subseteq \langle \alpha, \beta \rangle$, that is, $\varepsilon \in \mathrm{End}(\langle \alpha, \beta \rangle)$.

Discriminants

Let $f(x, y) = ax^2 + bxy + cy^2$ for some a, b, and c in $\mathbb{Q}$ as in (7.3), so that the discriminant D of f is $b^2 - 4ac$. By the quadratic formula,

$$\begin{aligned} f(x,y) &= a\Big(x - \frac{-b+\sqrt{D}}{2a}y\Big)\Big(x - \frac{-b-\sqrt{D}}{2a}y\Big) \\ &= \frac{1}{a}\Big(ax + \frac{b-\sqrt{D}}{2}y\Big)\Big(ax + \frac{b+\sqrt{D}}{2}y\Big). \end{aligned}$$

As before, $D = s^2 d$ for some nonzero rational s and some rational integer d that is square-free or zero. Assuming as on page 45 that d is square-free, but not 1, or equivalently, $\sqrt{D} \notin \mathbb{Q}$, we have $a \neq 0$, and again $f(x, y) = \mathrm{N}(\alpha x + \beta y)/a$, where $\alpha = a$, $\beta = (b+\sqrt{D})/2$, and the norm is computed in K, which is $\mathbb{Q}(\sqrt{d})$ (again as on page 45). Since $\sqrt{D}$ is irrational, we have $\beta/\alpha \notin \mathbb{Q}$, that is, α and β are linearly independent over $\mathbb{Q}$; equivalently, $\{\alpha, \beta\}$ is a basis of K as a vector space over $\mathbb{Q}$.

Now suppose conversely α and β are in K and f is given simply by $f(x, y) = \mathrm{N}(\alpha x + \beta y)$. Then

$$\begin{aligned} f(x,y) &= (\alpha x + \beta y)(\alpha' x + \beta' y) \\ &= \alpha\alpha' x^2 + (\alpha\beta' + \alpha'\beta)xy + \beta\beta' y^2 \end{aligned}$$

so that

$$D = (\alpha\beta' + \alpha'\beta)^2 - 4\alpha\beta\alpha'\beta' = (\alpha\beta' - \alpha'\beta)^2. \tag{9.2}$$

We note then

$$D = \begin{vmatrix} \alpha & \alpha' \\ \beta & \beta' \end{vmatrix}^2 . \tag{9.3}$$

Alternatively,

$$f(x,y) = \mathrm{N}(\alpha)\, x^2 + \mathrm{Tr}(\alpha\beta')xy + \mathrm{N}(\beta)\, y^2,$$
$$D = \mathrm{Tr}(\alpha\beta')^2 - 4\,\mathrm{N}(\alpha\beta).$$

Lemma 4. *For some elements α and β of K, let D be the discriminant of $\mathrm{N}(\alpha x + \beta y)$, so that $D = s^2 d$ for some s in $\mathbb{Q}$. The following are equivalent:*

(i) *$D \neq 0$;*
(ii) *α and β are linearly independent over $\mathbb{Q}$;*
(iii) *$\sqrt{D}$ is irrational.*

Proof. If $\alpha = 0$, then $D = 0$ by (9.2), so (i), (ii), and (iii) all fail. Suppose $\alpha \neq 0$. Then we can write β/α as $r + t\sqrt{d}$ for some r and t in $\mathbb{Q}$. From (9.2), we have

$$D = \left(\alpha\alpha'\Big(\frac{\beta'}{\alpha'} - \frac{\beta}{\alpha}\Big)\right)^2 = \mathrm{N}(\alpha)^2 \left(\Big(\frac{\beta}{\alpha}\Big)' - \Big(\frac{\beta}{\alpha}\Big)\right)^2$$
$$= \mathrm{N}(\alpha)^2 \cdot 4t^2 d = (2t\,\mathrm{N}(\alpha))^2 \cdot d.$$

Since $2t\,\mathrm{N}(\alpha) \in \mathbb{Q}$, we have

$$\sqrt{D} \in \mathbb{Q} \iff D = 0 \iff t = 0 \iff \beta/\alpha \in \mathbb{Q}.$$

Thus, (i), (ii), and (iii) are again equivalent. □

We have observed that two lattices $\langle \alpha, \beta \rangle$ and $\langle \gamma, \delta \rangle$ of K are the same lattice Λ if and only if

$$\begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

for some a, b, c, and d in $\mathbb{Z}$ such that $ad - bc = \pm 1$. In this case,

$$\begin{pmatrix} \gamma & \gamma' \\ \delta & \delta' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix},$$

so that

$$\begin{vmatrix} \gamma & \gamma' \\ \delta & \delta' \end{vmatrix}^2 = \begin{vmatrix} \alpha & \alpha' \\ \beta & \beta' \end{vmatrix}^2.$$

This number is the **discriminant** of Λ, and we write

$$\Delta(\Lambda) = \Delta(\alpha, \beta) = \begin{vmatrix} \alpha & \alpha' \\ \beta & \beta' \end{vmatrix}^2. \tag{9·4}$$

This is the discriminant of the quadratic forms $\mathrm{N}(\alpha x + \beta y)$ and $\mathrm{N}(\gamma x + \delta y)$, by (9.3).

Lemma 5. *Suppose $\alpha, \beta \in K$.*

(i) $\Delta(\alpha, \beta) \in \mathbb{Q}$;
(ii) $\alpha, \beta \in \mathfrak{O}_K \implies \Delta(\alpha, \beta) \in \mathbb{Z}$;
(iii) $\{\alpha, \beta\}$ *is a basis for K if and only if* $\Delta(\alpha, \beta) \neq 0$.

Proof. We have (i) by what we have just noted, and (iii) by Lemma 4. As for (ii), if $\alpha, \beta \in \mathfrak{O}_K$, then $\Delta(\alpha, \beta) \in \mathfrak{O}_K \cap \mathbb{Q}$, which is $\mathbb{Z}$ by an exercise. □

Quadratic form example

Suppose

$$f(x, y) = 2x^2 + 6xy + 3y^2.$$

Then $D = 36 - 24 = 12 = 2^2 \cdot 3$. Also

$$\begin{aligned} f(x,y) &= 2\Big(x^2 + 3xy + \frac{3}{2}y^2\Big) \\ &= 2\Big(x - \frac{-3+2\sqrt{3}}{2}y\Big)\Big(x - \frac{-3+2\sqrt{3}}{2}y\Big) \\ &= \frac{1}{2}\big(2x + (3+2\sqrt{3})y\big)\big(2x + (3-2\sqrt{3})y\big). \end{aligned}$$

So we have a bijection $(x,y) \mapsto 2x + (3+2\sqrt{3})y$ between the sets

$$\begin{aligned} &\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \colon f(x,y) = m\}, \\ &\{\xi \in \langle 2, 3+2\sqrt{3}\rangle \colon \mathrm{N}(\xi) = 2m\}, \end{aligned}$$

where the norm is computed in $\mathbb{Q}(\sqrt{3})$. We can write the form as a matrix product:

$$f(x,y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 3 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Then making a change of variable, as by

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix},$$

means forming a new product

$$\begin{pmatrix} u & v \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 3 & 3 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}.$$

Such a change may be useful particularly if what we want to understand is the possible values of $f(x,y)$.

Lattices

Again d and K are as on page 45, and ω, in (7.1) on page 48.

Lemma 6. *Let L be a subset of K. Then L is a lattice of K if and only if:*

(i) *L is an additive subgroup of K (that is, K contains 0 and is closed under addition and subtraction);*
(ii) *as a vector-space, K is spanned by L (over $\mathbb{Q}$);*
(iii) *$nL \subseteq \mathfrak{O}_K$ for some n in $\mathbb{Z} \smallsetminus \{0\}$.*

Proof. Suppose L is a lattice of K. Then (i) and (ii) hold by definition of lattice. Also $L = \langle \alpha, \beta \rangle$ for some α and β in K. But $\mathfrak{O}_K$ is the lattice $\langle 1, \omega \rangle$ by Theorem 11. In particular, $(1, \omega)$ spans K. So $\alpha = k + \ell\omega$ and $\beta = r + s\omega$ for some k, ℓ, r, and s in $\mathbb{Q}$. Let n be a common multiple of their denominators. Then $n\alpha$ and $n\beta$ are in $\mathfrak{O}_K$, so (iii) holds.

Suppose conversely that (i), (ii), and (iii) hold. Then L contains α and β such that $\{\alpha, \beta\}$ is a basis for K; and there is n in $\mathbb{Z} \smallsetminus \{0\}$ such that, for every such basis, $n\alpha$ and $n\beta$ are in $\mathfrak{O}_K$. By Lemma 5, this means $\Delta(n\alpha, n\beta) \in \mathbb{Z}$. Also $\Delta(\alpha, \beta) \neq 0$. So we may suppose α and β have been chosen from L so as to minimize $|\Delta(n\alpha, n\beta)|$, which is $n^4|\Delta(\alpha, \beta)|$. We shall show $L = \langle \alpha, \beta \rangle$. Suppose $\gamma \in L$. Then $\gamma \in K$, so

$$\gamma = \alpha r + \beta s$$

for some r and s in $\mathbb{Q}$. We want to show r and s are in $\mathbb{Z}$. Since

$$\gamma - \alpha[r] = \alpha(r - [r]) + \beta s,$$

we compute

$$\Delta(\gamma - \alpha[r], \beta) = (r - [r])^2 \Delta(\alpha, \beta),$$

since

$$\begin{vmatrix} \alpha(r-[r])+\beta s & \alpha'(r-[r])+\beta' s \\ \beta & \beta' \end{vmatrix}^2$$
$$= \begin{vmatrix} \alpha(r-[r]) & \alpha'(r-[r]) \\ \beta & \beta' \end{vmatrix}^2 = (r-[r])^2 \begin{vmatrix} \alpha & \alpha' \\ \beta & \beta' \end{vmatrix}^2 .$$

By minimality of $|\Delta(\alpha,\beta)|$, we must have $r-[r]=0$, so $r \in \mathbb{Z}$. By symmetry, $s \in \mathbb{Z}$. □

10. March 28, 2008 (Friday)

Orders and conductors

The ring $\mathrm{End}(\Lambda)$ is also called the **order** of Λ and denoted by

$$\mathfrak{O}_\Lambda.$$

By Lemma 3 (page 56), we know that this is a sub-ring of $\mathfrak{O}_K$, which is $\langle 1, \omega \rangle$ by Theorem 11 (page 48).

Lemma 7. *$\mathfrak{O}_\Lambda$ is also a lattice of K.*

Proof. By Lemma 6, it is enough to show that $\mathfrak{O}_\Lambda$ spans K over $\mathbb{Q}$. Write Λ as $\langle \alpha, \beta \rangle$. Let $\gamma \in K$. Then

$$\gamma \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

for some rational numbers r, s, t, and u. Let n be a common multiple of their denominators. Then $n\gamma\Lambda \subseteq \Lambda$, that is, $n\gamma \in \mathfrak{O}_\Lambda$. But $\gamma = (1/n)n\gamma$. □

Theorem 12. *For some positive rational integer c,*

$$\mathfrak{O}_\Lambda = \langle 1, c\omega \rangle. \tag{10.1}$$

Proof. We know $1 \in \mathfrak{O}_\Lambda$ and $\mathfrak{O}_\Lambda \subseteq \langle 1, \omega \rangle$. Since $\mathfrak{O}_\Lambda$ is a lattice, it must therefore have an irrational element $m + n\omega$, where m and n are rational integers and $n \neq 0$. Then $n\omega \in \mathfrak{O}_\Lambda$. Let c be the least positive such n. Then for *any* such n we have $\gcd(c, n)\omega \in \mathfrak{O}_\Lambda$, and so $c \mid n$. Now (10.1) follows. □

The number c is the **conductor** of $\mathfrak{O}_\Lambda$.

Theorem 13. *$\mathfrak{O}_{\gamma\Lambda} = \mathfrak{O}_\Lambda$ for all non-zero γ in K.*

Proof. Since $\xi \mapsto \gamma\xi$ is a bijection from K to itself,

$$\xi\Lambda \subseteq \Lambda \iff \xi\gamma\Lambda \subseteq \gamma\Lambda. \qquad \square$$

In looking for $\mathfrak{O}_\Lambda$, we may therefore assume that

$$\boxed{\Lambda \text{ is the lattice } \langle 1, \tau\rangle,}$$

where $\tau = \beta/\alpha$, so that also

$$a\tau^2 + b\tau + c = 0$$

for some a, b, and c in $\mathbb{Z}$, where $\gcd(a, b, c) = 1$ and $a > 0$. Then

$$a\tau^2 = -b\tau - c,$$

which shows $\langle 1, a\tau\rangle \subseteq \mathfrak{O}_\Lambda$. That this inclusion is an equality can be seen first in some examples. If $b = 0$ and $c = 1$, so $a\tau^2 = -1$, we may assume $\tau = \mathrm{i}/\sqrt{a}$, as in Figure 10.1. If

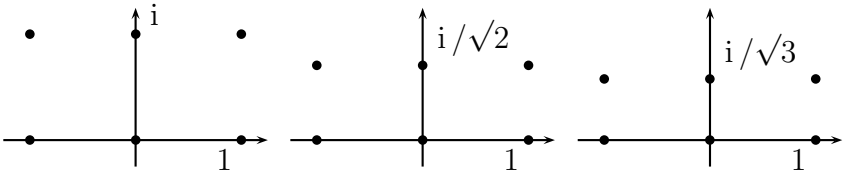

Figure 10.1.: Lattices $\langle 1, \mathrm{i}/\sqrt{a}\rangle$

$b = -1$ and $c = 1$, so $a\tau^2 = \tau - 1$, we may assume $\tau = (1 + \mathrm{i}\sqrt{4a - 1})/2a$, and again $|\tau| = 1/\sqrt{a}$, as in Figure 10.2.

Theorem 14. *$\mathfrak{O}_\Lambda = \langle 1, a\tau\rangle$.*

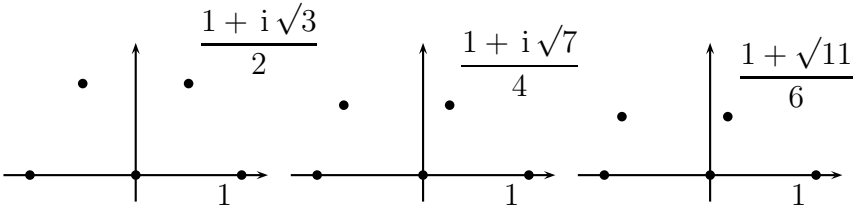

Figure 10.2.: Lattices $\langle 1, (1+\mathrm{i}\sqrt{4a-1})/2a\rangle$

Proof. We have first

$$\begin{aligned}\theta \in \mathfrak{O}_\Lambda &\iff \theta\langle 1,\tau\rangle \subseteq \langle 1,\tau\rangle \\ &\iff \theta \in \langle 1,\tau\rangle \ \ \&\ \ \theta\tau \in \langle 1,\tau\rangle.\end{aligned}$$

Any element θ of $\langle 1,\tau\rangle$ is $x+y\tau$ for some x and y in $\mathbb{Z}$, and then

$$\begin{aligned}\theta\tau \in \langle 1,\tau\rangle &\iff x\tau + y\tau^2 \in \langle 1,\tau\rangle \\ &\iff y\tau^2 \in \langle 1,\tau\rangle \\ &\iff \frac{yb}{a}\tau + \frac{yc}{a} \in \langle 1,\tau\rangle \\ &\iff a \mid yb \ \ \&\ \ a \mid yc \\ &\iff a \mid y.\end{aligned}$$

In short, $\theta \in \mathfrak{O}_\Lambda \iff \theta \in \langle 1, a\tau\rangle$. □

11. April 1, 2008 (Tuesday)

What then is the conductor of $\mathfrak{O}_\Lambda$? Since

$$\tau = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

but $\tau \in K$, we have

$$\sqrt{b^2 - 4ac} = s\sqrt{d} \tag{11.1}$$

for some s in $\mathbb{Z}$. This gives us

$$\mathfrak{O}_\Lambda = \left\langle 1, \frac{-b \pm s\sqrt{d}}{2} \right\rangle, \qquad b^2 \equiv s^2 d \pmod 4.$$

Theorem 15. *The conductor of $\mathfrak{O}_\Lambda$ is*

- *$s/2$, when $d \not\equiv 1 \pmod 4$,*
- *s, when $d \equiv 1 \pmod 4$,*

where s is as in (11.1).

Proof. If d is congruent to 2 or 3, then (since squares are congruent to 0 or 1), we must have $s^2 \equiv 0$, so s is even, and then b is even, so that

$$\mathfrak{O}_\Lambda = \left\langle 1, \frac{s}{2}\sqrt{d} \right\rangle = \left\langle 1, \frac{s}{2}\omega \right\rangle.$$

If $d \equiv 1$, then $s^2 \equiv b^2$, so $b \pm s$ is even, and hence

$$\mathfrak{O}_\Lambda = \left\langle 1, \frac{-b \mp s \pm s \pm s\sqrt{d}}{2} \right\rangle = \langle 1, s\omega \rangle. \qquad \square$$

To sum up the last four theorems:

- For the lattice Λ or $\langle \alpha, \beta \rangle$ of K, for some conductor c, the endomorphism ring $\mathfrak{O}_\Lambda$ is $\langle 1, c\omega \rangle$.
- We may replace Λ with $\langle 1, \tau \rangle$, where $\tau = \beta/\alpha$.
- If τ solves $ax^2 + bx + c = 0$, the coefficients having no common factor, then $\mathfrak{O}_\Lambda$ is $\langle 1, a\tau \rangle$.
- Moreover, $\mathfrak{O}_\Lambda$ is $\langle 1, s\boldsymbol{\omega}/2 \rangle$ or $\langle 1, s\boldsymbol{\omega} \rangle$, where d is not or is congruent to 1 *modulo* 4 respectively, and $s^2 d = b^2 - 4ac$.

Conversely, we have the following.

Theorem 16. *For every d, for every positive rational integer c, when $\tau = c\omega$, then $\mathfrak{O}_\Lambda = \Lambda$.*

Proof. Let $\tau = c\omega$.

- If $d \not\equiv 1 \pmod 4$, then $\tau^2 - c^2 d = 0$.
- If $d \equiv 1 \pmod 4$, then $\tau^2 - c\tau - c^2(d-1)/4 = 0$. □

Units

If, for some d, we can bring a quadratic Diophantine equation into the form

$$\mathrm{N}\,(x\alpha + y\beta) = m, \tag{11.2}$$

then its solutions correspond to the solutions from Λ of

$$\mathrm{N}\,(\xi) = m.$$

From any of the latter solutions, we obtain another by multiplying by a solution from $\mathfrak{O}_\Lambda$ of

$$\mathrm{N}\,(\eta) = 1.$$

Lemma 8. *The units of $\mathfrak{O}_\Lambda$, which itself is $\langle 1, c\omega\rangle$, are just those elements that solve $\mathrm{N}(\xi) = \pm 1$; and these are the elements $x + cwy$ such that, when $d \not\equiv 1$ and $d \equiv 1$ respectively* (mod 4),

$$x^2 - d(cy)^2 = \pm 1, \tag{11.3}$$

$$\left(x + \frac{cy}{2}\right)^2 - \frac{d}{4}(cy)^2 = \pm 1. \tag{11.4}$$

Proof. Since $\mathfrak{O}_\Lambda \subseteq \mathfrak{O}_K$, the norms of its elements are rational integers, by Theorem 10 (page 46). Suppose α is a unit of $\mathfrak{O}_\Lambda$. Then $\alpha \neq 0$ and $\alpha^{-1} \in \mathfrak{O}_\Lambda$. But $1 = \mathrm{N}(1) = \mathrm{N}(\alpha\alpha^{-1}) = \mathrm{N}(\alpha)\,\mathrm{N}(\alpha^{-1})$, and since these factors are in $\mathbb{Z}$, we have that $\mathrm{N}(\alpha)$ is a unit in $\mathbb{Z}$, that is, $\mathrm{N}(\alpha) = \pm 1$.

Suppose conversely $\alpha \in \mathfrak{O}_\Lambda$ and $\mathrm{N}(\alpha) = \pm 1$. This means $\alpha\alpha' = \pm 1$, so $\alpha^{-1} = \pm\alpha'$. But $\mathfrak{O}_\Lambda$ is closed under $\xi \mapsto \xi'$, since $\mathfrak{O}_\Lambda = \langle 1, c\omega\rangle$, and ω' is either $-\omega$ or $1 - \omega$. Therefore $\alpha^{-1} \in \mathfrak{O}_\Lambda$, so α is a unit of $\mathfrak{O}_\Lambda$. □

Imaginary case

The easier case to consider is $d < 0$, when $\mathrm{N}(\xi) = |\xi|^2$, which is not negative, so only the positive signs in (11.3) and (11.4) need be considered. In particular, all units of $\mathfrak{O}_\Lambda$ lie on the unit circle, as in Figure 11.1, which indeed shows all of the possibilities, by the following.

Theorem 17. *When $d < 0$, then the units of $\langle 1, c\omega\rangle$ are:*

(i) ± 1 *and* $\pm\omega$, *when* $c = 1$ *and* $d = -1$;
(ii) ± 1, $\pm\omega'$, *and* $\pm\omega$, *when* $c = 1$ *and* $d = -3$;
(iii) ± 1, *in all other cases.*

Proof. If $d \not\equiv 1$, then (11.3) has the solutions

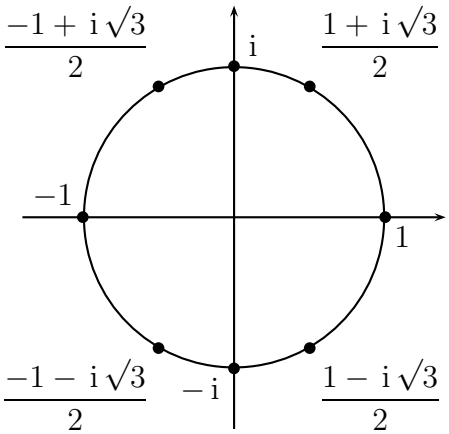

Figure 11.1.: Units in imaginary quadratic fields

(i) $(\pm 1, 0)$, if $c > 1$ or $d < -1$;
(ii) $(\pm 1, 0)$ and $(0, \pm 1)$, if $c = 1$ and $d = -1$.

If $d \equiv 1$, then either $d = -3$, or else $d \leqslant -7$. In the latter case, the only solutions to (11.4) are $(\pm 1, 0)$. But if $d = -3$, so that (11.4) becomes

$$x^2 + x \cdot cy + (cy)^2 = 1,$$

then the solutions are

(i) $(\pm 1, 0)$, if $c > 1$;
(ii) $(\pm 1, 0)$, $(\pm 1, \mp 1)$, and $(0, \pm 1)$, if $c = 1$. □

Problem 6. *Solve the quadratic Diophantine equation*

$$x^2 + xy + y^2 = 3. \tag{11.5}$$

Solution. We complete the square. Since

$$x^2 + xy + y^2 = x^2 + xy + \frac{1}{4}y^2 + \frac{3}{4}y^2,$$

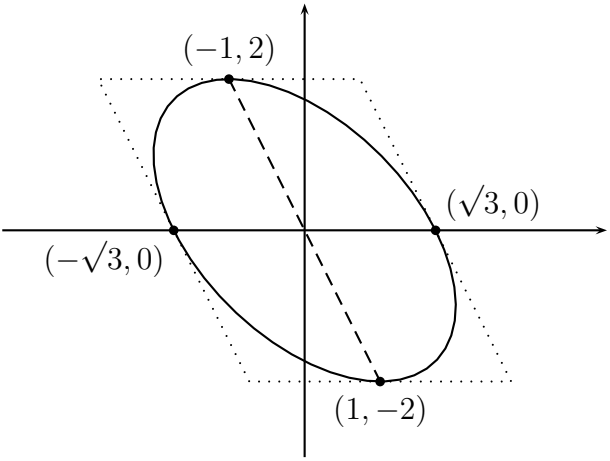

Figure 11.2.: Ellipse $\frac{1}{3}\left(x+\frac{1}{2}y\right)^2+\frac{1}{4}y^2=1$

we can rewrite (11.5) as

$$\left(x+\frac{y}{2}\right)^2+\frac{3}{4}y^2=3. \tag{11.6}$$

This defines the ellipse shown in Figure 11.2, of which each of the lines $y=2x$ and $y=0$ is a *diameter* (*διάμετρος*) that is *conjugate* (*συζυγής*) to the other in the sense of Apollonius ([2, I.16, p. 64] or [3]), namely that each of the lines bisects the chords of the ellipse that are parallel to the other line. The figure suggests where to look for the solutions to (11.5); they are

$$(\pm1,\pm1), \qquad (\mp1,\pm2), \qquad (\pm2,\mp1),$$

as shown in Figure 11.3.

Alternatively, instead of sketching an ellipse, we may just observe that $(1,1)$ is a solution to our equation. To find the

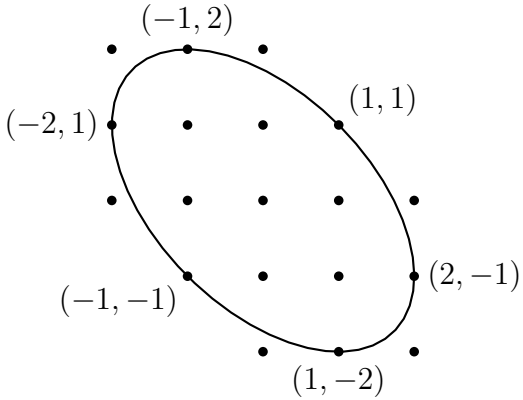

Figure 11.3.: Solutions of $x^2 + xy + y^2 = 3$

others, letting $d = -3$, we write (11.5) as

$$\mathrm{N}\,(x + \omega y) = 3.$$

Letting $\Lambda = \langle 1, \omega \rangle$, we have $\mathfrak{O}_\Lambda = \Lambda = \mathfrak{O}_K$, which by Theorem 17 has the six units ± 1, $\pm\omega$, and $\pm\omega'$, each having norm 1. Since $1 + \omega$ is a solution of

$$\mathrm{N}\,(\xi) = 3$$

from Λ, so are $\pm(1 + \omega)$, $\pm\omega(1 + \omega)$, and $\pm\omega'(1 + \omega)$. Since $\omega^2 - \omega + 1 = 0$, and $\omega + \omega' = 1$, these solutions are

$$\pm\,(1 + \omega), \qquad \pm\,(2\omega - 1), \qquad \pm\,(2 - \omega)$$

as in Figure 11.4, corresponding to the solutions to (11.5). It is now easy to see from Figure 11.4 that there are no other solutions. □

Problem 7. *Solve*

$$4x^2 + 2xy + y^2 = 7. \tag{11.7}$$

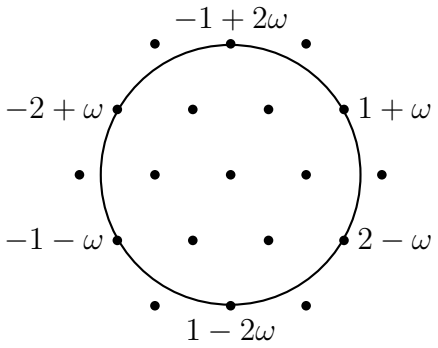

Figure 11.4.: Solutions of $\mathrm{N}(\xi) = 3$ from $\langle 1, \omega \rangle$ in $\mathbb{Q}(\sqrt{-3})$

Solution. We complete the square in y now, because it seems simpler, getting

$$3x^2 + (x+y)^2 = 7. \tag{11.8}$$

This defines the ellipse shown in Figure 11.5, with conjugate diameters $x = 0$ and $y = -x$. We find the integer points as shown in Figure 11.6.

Alternatively, one solution is $(1, 1)$. From (11.8), we factorize:

$$\begin{aligned} 3x^2 + (x+y)^2 &= (\sqrt{3}x + \mathrm{i}\,(x+y))(\sqrt{3}x - \mathrm{i}\,(x+y)) \\ &= ((\sqrt{3} + \mathrm{i}\,)x + \mathrm{i}\,y)((\sqrt{3} - \mathrm{i}\,)x - \mathrm{i}\,y), \end{aligned} \tag{11.9}$$

but this is not over a quadratic field, since a field that contains $\sqrt{3} + \mathrm{i}$ and i contains also $\sqrt{3}$, and $[\mathbb{Q}(\sqrt{3}, \mathrm{i}\,) : \mathbb{Q}] = 4$ as in Figure 11.7. We can fix this problem by multiplying each factor in (11.9) by the appropriate unit, such as $-\mathrm{i}$ and i. What amounts to the same thing is to perform the alternative

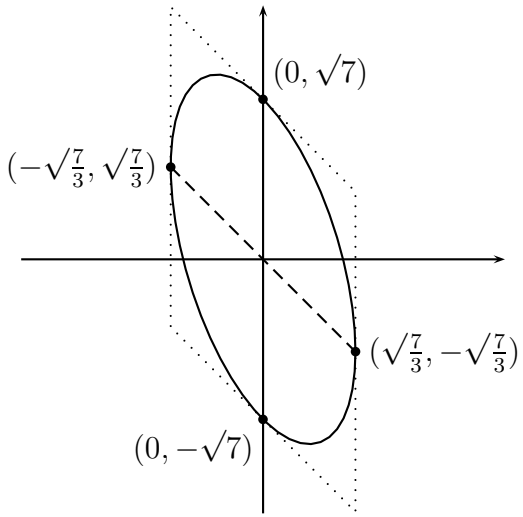

Figure 11.5.: Ellipse $\frac{3}{7}x^2 + \frac{1}{7}(x+y)^2 = 1$

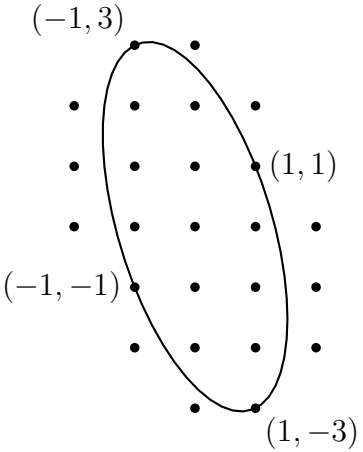

Figure 11.6.: Solutions to $4x^2 + 2xy + 1 = 7$

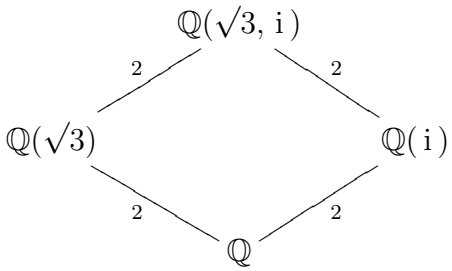

Figure 11.7.: Subfields of $\mathbb{Q}(\sqrt{3},\,\mathrm{i}\,)$

factorization

$$\begin{aligned} 3x^2 + (x+y)^2 &= (x+y)^2 + 3x^2 \\ &= (x+y+x\sqrt{-3})(x+y-x\sqrt{-3}), \end{aligned}$$

so that, letting $d = -3$, we can write (11.7) as

$$\mathrm{N}\,(y + 2\omega x) = 7.$$

Letting $\Lambda = \langle 1, 2\omega \rangle$, we want to solve

$$\mathrm{N}\,(\xi) = 7 \tag{11.10}$$

in Λ. We know one solution, namely $1 + 2\omega$. By Theorem 16, $\mathfrak{O}_\Lambda = \Lambda$. The only units of this are ± 1, by Theorem 17. Hence we have the solutions $\pm(1+2\omega)$ of (11.10). To find any others, again we can draw a picture, Figure 11.8. So (11.10) has the solutions $\pm(1 + 2\omega)$ and $\pm(3 - 2\omega)$ in $\langle 1, 2\omega \rangle$, but no others (though there are more solutions in $\langle 1, \omega \rangle$). The solutions of (11.7) are therefore $(\pm 1, \pm 1)$ and $(\mp 1, \pm 3)$ (as we already saw in Figure 11.6, if we cared to draw it). □

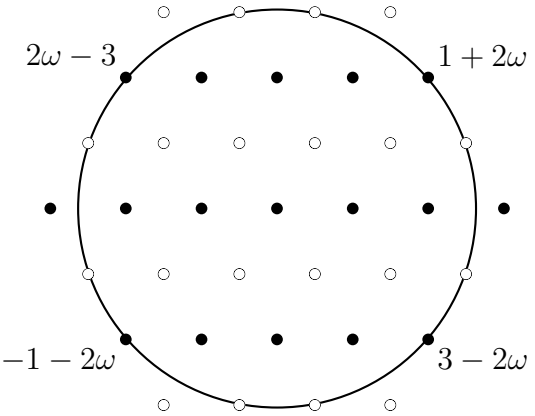

Figure 11.8.: Solutions of $\mathrm{N}(\xi) = 7$ from $\langle 1, 2\omega \rangle$ in $\mathbb{Q}(\sqrt{-3})$

In the same way, we can solve any quadratic Diophantine equation

$$ax^2 + bxy + cy^2 = m,$$

provided $b^2 - 4ac < 0$. For in this case, the equation defines an ellipse, which is bounded, so that there are only finitely many possible solutions to check.

Real case

Now we move to the case where $d > 0$, so $K \subseteq \mathbb{R}$. We have

$$\langle 1, c\sqrt{d} \rangle \subseteq \langle 1, c\omega \rangle = \mathfrak{O}_\Lambda.$$

A unit of $\mathfrak{O}_\Lambda$ of the form $x + cy\sqrt{d}$ thus corresponds to a solution of (11.3). Since a Pell equation has infinitely many solutions by Theorem 3, we conclude that $\mathfrak{O}_\Lambda$ has infinitely many units. We want to find them.

Suppose ε is a unit of $\mathfrak{O}_\Lambda$. Since there are infinitely many units, there are units other than ± 1. So we may assume $\varepsilon \neq$

± 1. If $\varepsilon < 0$, then $-\varepsilon$ is a unit greater than 0. So we may assume $\varepsilon > 0$. If $0 < \varepsilon < 1$, then ε^{-1} is a unit greater than 1. So we may assume $\varepsilon > 1$. Also $\varepsilon < n$ for some n. But

$$\varepsilon^2 - (\varepsilon + \varepsilon')\varepsilon + \varepsilon\varepsilon' = 0,$$

that is, $\varepsilon^2 - \mathrm{Tr}(\varepsilon)\varepsilon + \mathrm{N}(\varepsilon) = 0$. Since $\pm 1 = \mathrm{N}(\varepsilon) = \varepsilon\varepsilon'$, we have $|\varepsilon'| = \varepsilon^{-1}$. Hence

$$|\mathrm{Tr}(\varepsilon)| = |\varepsilon + \varepsilon'| \leqslant \varepsilon + \varepsilon^{-1} < n + 1.$$

This shows that there are only finitely many possibilities for the equation $x^2 - \mathrm{Tr}(\varepsilon)x + \mathrm{N}(\varepsilon) = 0$. Hence there are only finitely many units of $\mathfrak{O}_\Lambda$ between 1 and n. Therefore there is a least such unit, the **fundamental unit,** which we may denote by

$$\varepsilon_\Lambda.$$

Then $({\varepsilon_\Lambda}^n : n \in \mathbb{Z})$ is an increasing sequence,

$$\lim_{n\to\infty} {\varepsilon_\Lambda}^n = \infty, \qquad \lim_{n\to-\infty} {\varepsilon_\Lambda}^n = 0.$$

Theorem 18. *When $d > 0$, each unit of $\mathfrak{O}_\Lambda$ is $\pm{\varepsilon_\Lambda}^n$ for some n in $\mathbb{Z}$. If $\mathrm{N}(\varepsilon_\Lambda) = 1$, then every unit has norm 1. If $\mathrm{N}(\varepsilon_\Lambda) = -1$, then the units of norm 1 are $\pm{\varepsilon_\Lambda}^{2n}$.*

Proof. We argue as in the proof of Theorem 3 (page 31), though more easily. Suppose ζ is a positive unit of $\mathfrak{O}_\Lambda$. Then

$${\varepsilon_\Lambda}^n \leqslant \zeta < {\varepsilon_\Lambda}^{n+1}$$

for some n. Hence $1 \leqslant {\varepsilon_\Lambda}^{-n}\zeta < \varepsilon_\Lambda$. But ${\varepsilon_\Lambda}^{-n}\zeta$ is a unit too. By minimality of ε_Λ, we conclude that $\zeta = {\varepsilon_\Lambda}^n$. □

How do we find ε_Λ?

Lemma 9. *Assuming $d > 0$, let ε be a unit $x + y\omega$ of $\mathfrak{O}_K$ such that $\varepsilon > 1$. Then both x and y are positive, or else $d = 5$ and $\varepsilon = \omega$.*

Proof. We have

$$(\omega - \omega')y = \varepsilon - \varepsilon' \geqslant \varepsilon - |\varepsilon^{-1}| > 0,$$

and $\omega > \omega'$, so $y > 0$. Also

$$1 > |\varepsilon'| = |x + y\omega'|;$$

so since $\omega' < 0$, and hence $y\omega' < 0$, we must have $x \geqslant 0$, since $x \in \mathbb{Z}$. If $x > 0$, we are done. Suppose $x = 0$. Then

$$\pm 1 = \mathrm{N}\,(y\omega) = \begin{cases} -dy^2, & \text{if } d \not\equiv 1 \pmod 4; \\ \dfrac{1-d}{4}y^2, & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

The only way this can happen is if $d = 5$ and $y = 1$ (since $y > 0$). □

12. April 4, 2008 (Friday)

Golden ratio

When $d = 5$, then $\omega = \phi$, the so-called **Golden Ratio:**

$$\phi = \frac{1 + \sqrt{5}}{2}.$$

This has an intimate connexion with the sequence $(\mathrm{F}_n \colon n \in \omega)$ of **Fibonacci numbers,** given by

$$\mathrm{F}_0 = 0, \quad \mathrm{F}_1 = 1, \quad \mathrm{F}_{n+2} = \mathrm{F}_n + \mathrm{F}_{n+1}.$$

We can continue the sequence backwards by writing the last rule as

$$\mathrm{F}_{n-2} = \mathrm{F}_n - \mathrm{F}_{n-1}.$$

Then the bi-directional sequence is

$$\ldots 13,\ -8,\ 5,\ -3,\ 2,\ -1,\ 1,\ 0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13 \ldots$$

Theorem 19. *The units of the ring of integers of* $\mathbb{Q}(\sqrt{5})$ *are* $\pm\phi^n$*; and*

$$\phi^n = \mathrm{F}_{n-1} + \mathrm{F}_n\phi. \tag{12.1}$$

Proof. Let $K = \mathbb{Q}(\sqrt{5})$. By Lemma 9, ϕ is the least unit of $\mathfrak{O}_K$ that is greater than 1. Then every unit is $\pm\phi^n$ for some n in $\mathbb{Z}$, by Theorem 18. Trivially (12.1) holds when $n = 1$. Also, since

$$\phi^2 = 1 + \phi, \tag{12.2}$$

we have

$$(x + y\phi)\phi = x\phi + y\phi^2 = y + (x + y)\phi. \tag{12.3}$$

Hence, if (12.1) holds when $n = k$, then

$$\phi^{k+1} = (\mathrm{F}_{k-1} + \mathrm{F}_k\phi)\phi = \mathrm{F}_k + (\mathrm{F}_{k-1} + \mathrm{F}_k)\phi = \mathrm{F}_k + \mathrm{F}_{k+1}\phi,$$

so (12.1) holds when $n = k + 1$. Therefore it holds for all positive n. Moreover, since

$$\phi^{-1} = \phi - 1,$$

we have

$$\begin{aligned}(x + y\phi)\phi^{-1} &= (x + y\phi)(\phi - 1)\\ &= -x + y\phi^2 + (x - y)\phi = y - x + x\phi,\end{aligned}$$

so that if (12.1) holds when $n = k$, it holds when $n = k-1$. □

13. April 8, 2008 (Tuesday)

Real example

Problem 8. *Solve the quadratic Diophantine equation*

$$4x^2 + 2xy - y^2 = 4. \tag{13.1}$$

Solution. Completing the square, we can rewrite the left member of the equation as either of

$$\left(2x + \frac{1}{2}y\right)^2 - \frac{5}{4}y^2, \qquad (2x + y\phi)(2x + y\phi'). \tag{13.2}$$

Thus (13.1) defines an hyperbola with *transverse* ($\pi\lambda\alpha\gamma\acute{\iota}\alpha$) diameter $y = 0$ and *upright* ($\grave{o}\rho\theta\acute{\iota}\alpha$) diameter $2x + \frac{1}{2}y = 0$, each of the lines $2x + y\phi = 0$ and $2x + y\phi' = 0$ being an asymptote ($\grave{a}\sigma\acute{\upsilon}\mu\pi\tau o\tau o\varsigma$), as in Figure 13.1. We may note the indicated integer points; but there may be infinitely many others, and we need a system for finding them.

Letting $d = 5$, we can write (13.1) as

$$\mathrm{N}\,(2x + y\phi) = 4.$$

Letting $\Lambda = \langle 2, \phi\rangle$, we have $\mathfrak{O}_\Lambda = \mathrm{End}(\langle 1, \phi/2\rangle)$ by Theorem 13. Since

$$4\left(\frac{\phi}{2}\right)^2 - 2 \cdot \frac{\phi}{2} - 1 = 0,$$

we have by Theorem 14 that $\mathfrak{O}_\Lambda = \langle 1, 2\phi\rangle$. Since $\mathrm{N}\,(\phi) = -1$, the positive elements of $\mathfrak{O}_\Lambda$ of norm 1 are the powers of the

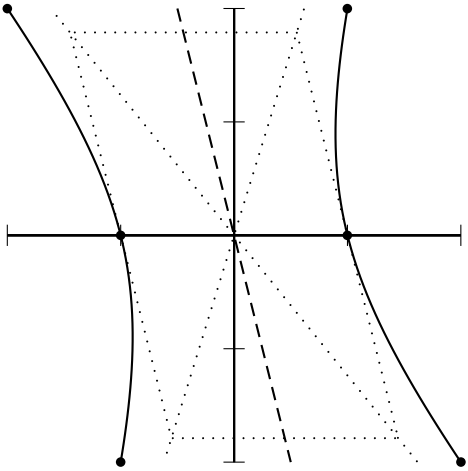

Figure 13.1.: Hyperbola $(2x + \frac{1}{2}y)^2 - \frac{5}{4}y^2 = 4$

least power ϕ^{2n}, where $n > 0$, that belongs to $\langle 1, 2\phi \rangle$. By Theorem 19, we have the following values.

n	2	4	6
ϕ^n	$1 + \phi$	$2 + 3\phi$	$5 + 8\phi$

So every element of $\mathfrak{O}_\Lambda$ of norm 1 is $\pm(5 + 8\phi)^n$ for some n in $\mathbb{Z}$. This means, if γ is a solution from Λ of

$$\mathrm{N}\,(\xi) = 4, \tag{13.3}$$

then so is $\pm(5 + 8\phi)^n\gamma$. There is some n in $\mathbb{Z}$ such that

$$(5 + 8\phi)^n < |\gamma| < (5 + 8\phi)^{n+1},$$

so that

$$1 < (5 + 8\phi)^{-n}|\gamma| < 5 + 8\phi.$$

Let $(5+8\phi)^{-n}|\gamma| = 2k+\ell\phi$. Then (k,ℓ) lies between the lines

$$2x + y\phi = 1, \qquad\qquad 2x + y\phi = 5 + 8\phi.$$

shown in Figure 13.2. These are parallel to one of the asymptotes of the hyperbola that we have discussed, and (k,ℓ) lies on this hyperbola, which, from the equation involving the second entry in (13.2), meets the bounding line $2x + y\phi = 1$ at this line's intersection with the line $2x + y\phi' = 4$, parallel to the other asymptote. This means (k,ℓ) lies within the parallelogram in the figure.

There are finitely many integer points in that parallelogram; for every such point (x,y), we compute $\mathrm{N}\,(2x + y\phi)$. In fact, once we have computed the norms indicated in the figure, we can see that the only points for which the corresponding norm is 4 are $(1,0)$, $(1,2)$, and $(2,6)$. Therefore the solutions to (13.1) are those (x,y) such that $2x + y\phi = \pm(5 + 8\phi)^n\gamma$, where $n \in \mathbb{Z}$ and $\gamma \in \{2, 2+2\phi, 4+6\phi\}$. The analysis continues in the next lecture. □

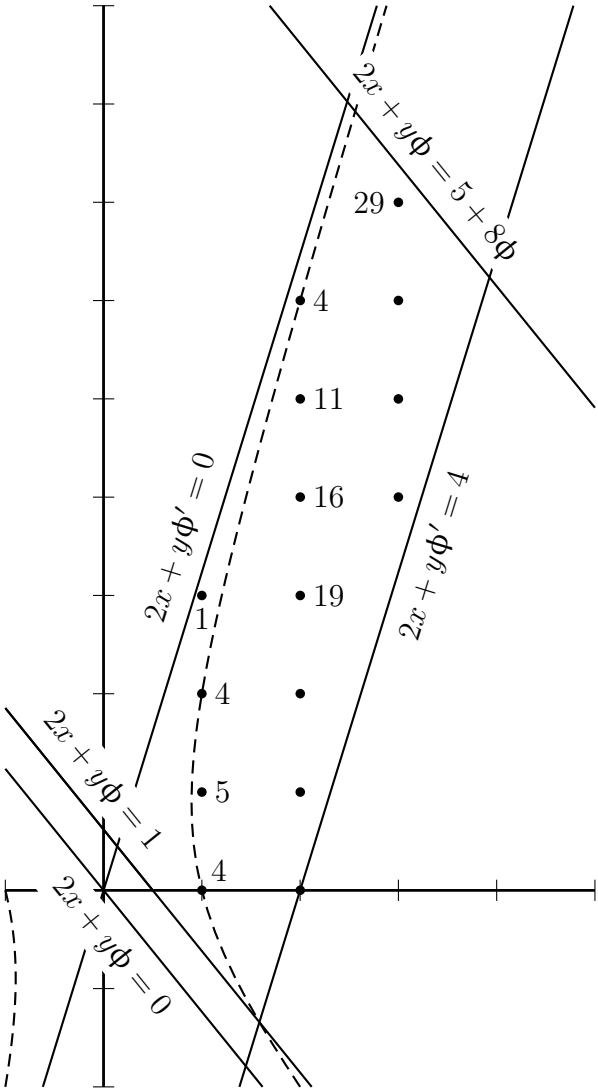

Figure 13.2.: Small solutions of $4x^2 + 2xy - y^2 = 4$

14. April 11, 2008 (Friday)

Example continued

At the end of the solution of Problem 8,

$$\{2, 2+2\phi, 4+6\phi\} = \{2\phi^0, 2\phi^2, 2\phi^4\}.$$

Thus the solutions to (13.3) are $\pm 2\phi^{2k}$, where $k \in \mathbb{Z}$. By Theorem 19, these solutions are

$$\pm(2\mathrm{F}_{2k-1} + 2\mathrm{F}_{2k}\phi).$$

Every Fibonacci number appears among them.

Under the correspondence $(x, y) \mapsto 2x + y\phi$ between solutions to (13.1) and solutions from $\langle 2, \phi \rangle$ to (13.3), the solutions of the former, shown in Figure 14.1, are $(\pm\mathrm{F}_{2k-1}, \pm 2\mathrm{F}_{2k})$. As suggested in the figure, we can form these into the single bi-directional sequence listed in Table 14.1. In particular, the sequence is $(a_n \colon n \in \mathbb{Z})$, where

$$a_n = \begin{cases} (\mathrm{F}_{-(4m+1)}, 2\mathrm{F}_{-4m}), & \text{if } n = 4m, \\ (\mathrm{F}_{4m+1}, 2\mathrm{F}_{4m+2}), & \text{if } n = 4m+1, \\ (-\mathrm{F}_{-(4m+3)}, -2\mathrm{F}_{-(4m+2)}), & \text{if } n = 4m+2, \\ (-\mathrm{F}_{4m+3}, -2\mathrm{F}_{4m+4}), & \text{if } n = 4m+3. \end{cases}$$

Alternatively, if $n = 4m + 2e + f$, where e and f are 0 or 1, then

$$a_n = ((-1)^e \mathrm{F}_{-(-1)^f(4m+2e+1)}, (-1)^e 2\mathrm{F}_{-(-1)^f(4m+2e+2f)}).$$

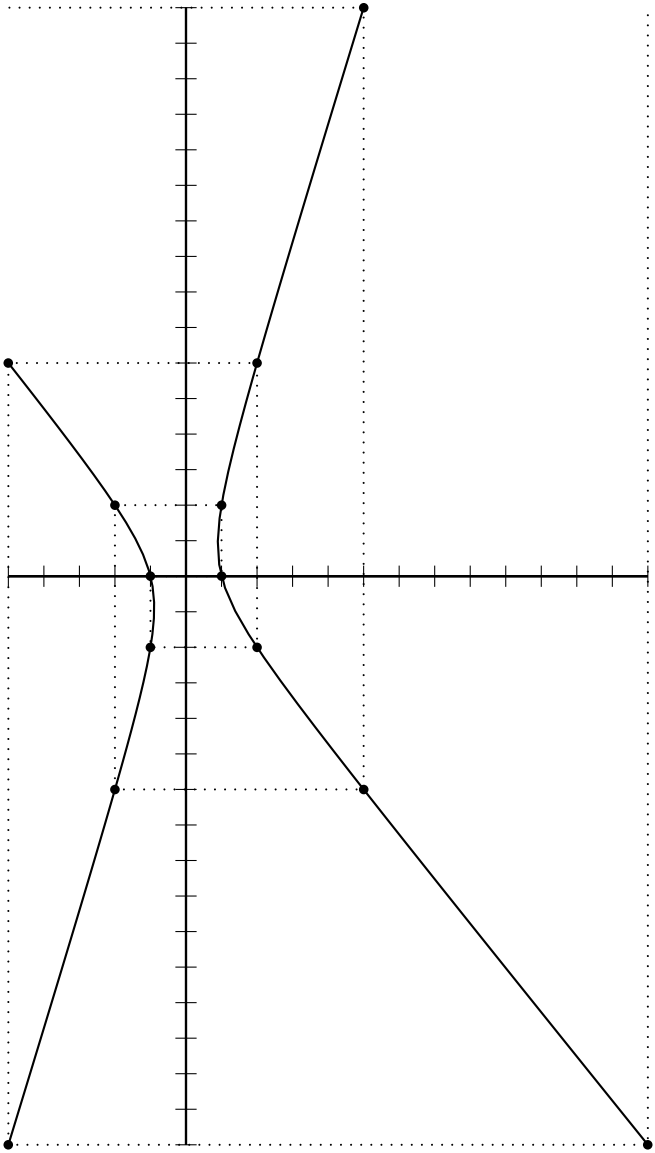

Figure 14.1.: Solutions of $4x^2 + 2xy - y^2 = 4$

$2x + y\phi$	(x, y)	
.....		
$2\phi^{-6}$	$(13, -16)$	$(\mathrm{F}_{-7}, 2\mathrm{F}_{-6})$
$-2\phi^{-(-6)}$	$(-5, -16)$	$(-\mathrm{F}_{-(-5)}, -2\mathrm{F}_{-(-6)})$
$-2\phi^{-4}$	$(-5, 6)$	$(-\mathrm{F}_{-5}, -2\mathrm{F}_{-4})$
$2\phi^{-(-4)}$	$(2, 6)$	$(\mathrm{F}_{-(-3)}, 2\mathrm{F}_{-(-4)})$
$2\phi^{-2}$	$(2, -2)$	$(\mathrm{F}_{-3}, 2\mathrm{F}_{-2})$
$-2\phi^{-(-2)}$	$(-1, -2)$	$(-\mathrm{F}_{-(-1)}, -2\mathrm{F}_{-(-2)})$
$-2\phi^{0}$	$(-1, 0)$	$(-\mathrm{F}_{-1}, -2\mathrm{F}_{0})$
$2\phi^{-0}$	$(1, 0)$	$(\mathrm{F}_{-1}, 2\mathrm{F}_{-0})$
$2\phi^{2}$	$(1, 2)$	$(\mathrm{F}_{1}, 2\mathrm{F}_{2})$
$-2\phi^{-2}$	$(-2, 2)$	$(-\mathrm{F}_{-3}, -2\mathrm{F}_{-2})$
$-2\phi^{4}$	$(-2, -6)$	$(-\mathrm{F}_{3}, -2\mathrm{F}_{4})$
$2\phi^{-4}$	$(5, -6)$	$(\mathrm{F}_{-5}, 2\mathrm{F}_{-4})$
$2\phi^{6}$	$(5, 16)$	$(\mathrm{F}_{5}, 2\mathrm{F}_{6})$
.....		

Table 14.1.: Solutions of $4x^2 + 2xy - y^2 = 4$

One can understand Theorem 19 in terms of matrices. By (12.3), multiplication in $\langle 1, \phi \rangle$ by ϕ corresponds, under the map

$$x + y\phi \mapsto \begin{pmatrix} x \\ y \end{pmatrix},$$

to the multiplication given by

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x + y \end{pmatrix}.$$

Inverting the square matrix, we have

$$\begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y - x \\ x \end{pmatrix},$$

corresponding to multiplication by ϕ^{-1}. Since

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

the solutions to (13.3) correspond to the matrices

$$\pm 2 \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{2n}.$$

15. April 15, 2008 (Tuesday)

Units from convergents

By converting a quadratic Diophantine equation to the form (11.2), we can solve as in Problems 6, 7, and 8, provided we can find the units of $\mathfrak{O}_K$. The case where $d > 0$ is the challenge. We need to find the fundamental unit ε_Λ, so that, by Theorem 18, every unit of $\mathfrak{O}_K$ is $\pm{\varepsilon_\Lambda}^n$ for some n.

We have solved this problem when $d = 5$, since then $\varepsilon_\Lambda = \phi$ by Theorem 19.

We know by Lemma 9 that $\varepsilon_\Lambda = a + b\omega$ for some positive a and b, unless $d = 5$.

- If $d \not\equiv 1 \pmod 4$, then $a + b\omega = a + b\sqrt{d}$.
- If $d \equiv 1$, then $a + b\omega = \frac{1}{2}(2a + b) + \frac{1}{2}b\sqrt{d}$.

For the moment writing $a+b\omega$ as $a'+b'\sqrt{d}$, we shall show that a'/b' is a convergent of $\sqrt{d}$. However, the argument will depend on a and b separately and thus on whether $d \equiv 1 \pmod 4$; also on how big d is. In any case, assuming $\sqrt{d} = [a_0; a_1, a_2, \dots]$, we let p_n/q_n be the nth convergent, $[a_0; a_1, \dots, a_n]$.

Lemma 10. *If a and b are rational integers such that*

$$1 \leqslant b < q_{n+1},$$

then

$$|p_n - q_n\sqrt{d}| \leqslant |a - b\sqrt{d}|.$$

Proof. By Theorem 2,

$$(-1)^n = p_{n+1}q_n - p_nq_{n+1} = \begin{vmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{vmatrix},$$

so the matrix is invertible, and there are s and t in $\mathbb{Z}$ such that

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{pmatrix} \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} sp_{n+1} + tp_n \\ sq_{n+1} + tq_n \end{pmatrix}.$$

We compute $a = sp_{n+1} + tp_n$ and $b = sq_{n+1} + tq_n$, so

$$a - b\sqrt{d} = s(p_{n+1} - q_{n+1}\sqrt{d}) + t(p_n - q_n\sqrt{d}).$$

It is enough to show that the two terms here have the same sign and $t \neq 0$. Since the factors $p_{n+1} - q_{n+1}\sqrt{d}$ and $p_n - q_n\sqrt{d}$ have opposite sign, it is enough to show $st \leqslant 0$ and $t \neq 0$. For the latter, we note

$$\begin{pmatrix} s \\ t \end{pmatrix} = (-1)^n \begin{pmatrix} q_n & -p_n \\ -q_{n+1} & p_{n+1} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix},$$

so

$$t = (-1)^n(-aq_{n+1} + bp_{n+1}).$$

Since $\gcd(p_{n+1}, q_{n+1}) = 1$, if $t = 0$, so that $aq_{n+1} = bp_{n+1}$, then $q_{n+1} \mid b$, hence $q_{n+1} \leqslant b$, contrary to our assumption.

To show $st \leqslant 0$, suppose $s \neq 0$. We have

$$b = sq_{n+1} + tq_n.$$

- If $s < 0$, then $t > 0$, since $1 \leqslant b$;
- if $s > 0$, then $t < 0$, since $b < q_{n+1}$. □

The lemma uses only that $\sqrt{d}$ has convergents up to step $n + 1$. The following lemma requires that all convergents of $\sqrt{d}$ exist, that is, $\sqrt{d}$ must be irrational.

Lemma 11. *If a and b are positive rational integers such that*

$$\left|\frac{a}{b} - \sqrt{d}\right| < \frac{1}{2b^2}, \tag{15.1}$$

then a/b is a convergent of $\sqrt{d}$.

Proof. Since $(q_n \colon n \in \omega)$ increases to ∞, we can find n such that

$$q_n \leqslant b < q_{n+1}.$$

In this case, by Lemma 10 and (15.1),

$$q_n\left|\frac{p_n}{q_n} - \sqrt{d}\right| \leqslant b\left|\frac{a}{b} - \sqrt{d}\right| < \frac{1}{2b},$$

so that

$$\left|\frac{p_n}{q_n} - \sqrt{d}\right| < \frac{1}{2bq_n}.$$

By the triangle inequality and this,

$$\begin{aligned}\frac{1}{bq_n}|aq_n - bp_n| = \left|\frac{a}{b} - \frac{p_n}{q_n}\right| &\leqslant \left|\frac{a}{b} - \sqrt{d}\right| + \left|\sqrt{d} - \frac{p_n}{q_n}\right| \\ &< \frac{1}{2b^2} + \frac{1}{2bq_n} \leqslant \frac{1}{bq_n}.\end{aligned}$$

Thus $|aq_n - bp_n| < 1$, hence $aq_n = bp_n$ and $a/b = p_n/q_n$. □

Theorem 20. *Assuming $d > 0$, let $a + b\omega$ be a unit of $\mathfrak{O}_K$ where a and b are positive.*

(i) *If $d \not\equiv 1 \pmod 4$, then a/b is a convergent of $\sqrt{d}$.*

(ii) *If $d \equiv 1$, then $(2a+b)/b$ is a convergent of $\sqrt{d}$, provided d is at least 21.*

Proof. (i) Suppose first

$$a^2 - db^2 = \pm 1, \tag{15.2}$$

which is the case when $d \not\equiv 1$. By Lemma 11, it is enough to show

$$\left|\frac{a}{b} - \sqrt{d}\right| < \frac{1}{2b^2},$$

that is,

$$|a - b\sqrt{d}| < \frac{1}{2b},$$

that is, multiplying by $a + b\sqrt{d}$ and using (15.2),

$$1 < \frac{a + b\sqrt{d}}{2b} = \frac{1}{2}\Big(\frac{a}{b} + \sqrt{d}\Big). \tag{15.3}$$

But we have, again from (15.2), and since $d \geqslant 2$,

$$\begin{aligned} a^2 - db^2 &\geqslant -1, \\ \Big(\frac{a}{b}\Big)^2 &\geqslant d - \frac{1}{b^2} \geqslant d - 1, \qquad (15.4) \\ \frac{a}{b} &\geqslant \sqrt{d-1}, \\ \frac{1}{2}\Big(\frac{a}{b} + \sqrt{d}\Big) &\geqslant \frac{1}{2}(\sqrt{d-1} + \sqrt{d}) > 1, \qquad (15.5) \end{aligned}$$

which gives us (15.3).

(ii) In case $d \equiv 1$, we try to proceed likewise. Parallel to (15.2) we have

$$(2a + b)^2 - db^2 = \pm 4,$$

so that, parallel to (15.4),

$$\Big(\frac{2a + b}{b}\Big)^2 \geqslant d - \frac{4}{b^2} \geqslant d - 4. \tag{15.6}$$

We should like to show, parallel to (15.5),

$$\frac{1}{2}\Big(\frac{2a+b}{b}+\sqrt{d}\Big)>4. \tag{15.7}$$

It is enough if we can show

$$\frac{1}{2}(\sqrt{d-4}+\sqrt{d})>4. \tag{15.8}$$

We have this if $d \geqslant 21$. □

It remains to consider the cases when d is 17 or 13.

Lemma 12. *In Theorem 20, a is the nearest integer to $-b\omega'$.*

Proof. Since $a+b\omega > 2$ and $1 = (a+b\omega)|a+b\omega'|$, we conclude

$$|a+b\omega'| < \frac{1}{2},$$

so a is indeed the nearest integer to $-b\omega'$. □

Theorem 21. *Theorem 20 holds also when $d = 17$.*

Proof. In this case $-\omega' \approx 1.56$, to which 2 is nearest. Since $\mathrm{N}\,(2+\omega) = 2$, we must have $b > 1$. In the proof of Theorem 20, instead of (15.6) we have

$$\Big(\frac{2a+b}{b}\Big)^2 \geqslant d - \frac{4}{b^2} \geqslant d-1.$$

It is now enough if

$$\frac{1}{2}(\sqrt{d-1}+\sqrt{d})>4;$$

and we have this. □

Lemma 13. *If $d = 13$, then the fundamental unit of $\mathfrak{O}_K$ is $1 + \omega$, and $(2 + 1)/1$ is the first convergent of $\sqrt{13}$.*

Proof. We have $-\omega' \approx 1.3$, to which 1 is the nearest integer; and $1+\omega$ is indeed a unit (of norm -1) and is the least possible unit greater than 1, so it is the fundamental unit of $\mathfrak{O}_K$. □

16. April 18, 2008 (Friday)

The cases of 13 and 5

The argument for Case (ii) of Theorem 20 does not work when $d = 13$, because 13 is too small. We cannot show (15.7) in this case, because we have not got (15.8). However, we have (8.3), namely $\sqrt{13} = [3; 1, 1, 1, 1, 6]$, and from this we obtain the convergents listed in Table 16.1. To complete the table, noting that, by Lemma 13, the positive units of $\mathfrak{O}_K$ (when $d = 13$) are the powers of $1 + \omega$, we have

$$\omega = \frac{1+\sqrt{13}}{2}, \qquad \left(\omega - \frac{1}{2}\right)^2 = \frac{13}{4}, \qquad \omega^2 = 3 + \omega,$$

so that

$$\begin{aligned}(x + y\omega)(1 + \omega) &= x + (x + y)\omega + y\omega^2 \\ &= x + (x + y)\omega + y(3 + \omega) = x + 3y + (x + 2y)\omega.\end{aligned}$$

This gives the rest of Table 16.1. We show now that the pattern of the table continues.

Theorem 22. *Assuming $d = 13$, let p_k/q_k be the kth convergent of $\sqrt{d}$, and let*

$$a_\ell + b_\ell\omega = (1 + \omega)^\ell.$$

Then

$$\frac{2a_{3m+i} + b_{3m+i}}{b_{3m+i}} = \begin{cases} p_{5m}/q_{5m}, & \text{if } i = 1; \\ p_{5m+3}/q_{5m+3}, & \text{if } i = 2; \\ p_{5m+4}/q_{5m+4}, & \text{if } i = 3. \end{cases}$$

n	0	1	2	3	4
$\frac{p_n}{q_n}$	$\frac{3}{1}$	$\frac{4}{1}$	$\frac{7}{2}$	$\frac{11}{3}$	$\frac{18}{5}$
${p_n}^2 - 13{q_n}^2$	-4	3	-3	4	-1
$\frac{2a+b}{b}$	$\frac{3}{1}$			$\frac{11}{3}$	$\frac{36}{10}$
$(1+\omega)^k$ or $a+b\omega$	$1+\omega$			$4+3\omega$	$13+10\omega$
k	1			2	3

n	5	6	7	8	9
$\frac{p_n}{q_n}$	$\frac{119}{33}$	$\frac{137}{38}$	$\frac{256}{71}$	$\frac{393}{109}$	$\frac{649}{180}$
${p_n}^2 - 13{q_n}^2$	4	-3	3	-4	1
$\frac{2a+b}{b}$	$\frac{119}{33}$			$\frac{393}{109}$	$\frac{1298}{360}$
$(1+\omega)^k$ or $a+b\omega$	$43+33\omega$			$142+109\omega$	$469+360\omega$
k	4			5	6

Table 16.1.: Convergents and units when $d = 13$

Proof. We shall use the method of Problem 5 on page 57. From Table 16.1, our claim holds when $m = 0$. Writing p/q for p_k/q_k and p'/q' for p_{k+5}/q_{k+5}, we have

$$\begin{aligned}\frac{p'}{q'} &= \left[3;1,1,1,1,3+\frac{p}{q}\right] = \left[3;1,1,1,1+\frac{q}{p+3q}\right] \\ &= \left[3;1,1,1+\frac{p+3q}{p+4q}\right] = \left[3;1,1+\frac{p+4q}{2p+7q}\right] \\ &= \left[3;1+\frac{2p+7q}{3p+11q}\right] = 3+\frac{3p+11q}{5p+18q} = \frac{18p+65q}{5p+18q}.\end{aligned}$$

Writing $a + b\omega$ for $a_\ell + b_\ell\omega$, and $a' + b'\omega$ for $a_{\ell+3} + b_{\ell+3}\omega$, we have

$$\begin{aligned}a'+b'\omega &= (a+b\omega)(13+10\omega) \\ &= 13a + (10a+13b)\omega + 10b(3+\omega) \\ &= 13a+30b+(10a+23b)\omega.\end{aligned}$$

Therefore, if, as an inductive hypothesis, we have

$$\frac{2a+b}{b} = \frac{p}{q},$$

so that

$$\frac{a}{b} = \frac{p-q}{2q},$$

then

$$\begin{aligned}\frac{2a'+b'}{b'} &= \frac{26a+60b+10a+23b}{10a+23b} = \frac{36a+83b}{10a+23b} \\ &= \frac{36(p-q)+83\cdot 2q}{10(p-q)+23\cdot 2q} = \frac{36p+130q}{10p+36q} = \frac{18p+65q}{5p+18q} = \frac{p'}{q'}.\end{aligned}$$

Therefore the claim holds for all m. □

We know now that, when $d > 5$, if $s + t\sqrt{d}$ is a unit of $\mathfrak{O}_K$ with positive coefficients, then s/t is a convergent of $\sqrt{d}$. By the last theorem, not every convergent arises in this way when $d = 13$. It does when $d = 5$, by Theorem 19 and the next theorem; but then not every unit gives rise to a convergent.

Theorem 23. *The nth convergent of* $\sqrt{5}$ *is*

$$\frac{2\mathrm{F}_{3n+2} + \mathrm{F}_{3n+3}}{\mathrm{F}_{3n+3}}.$$

Proof. This can be left as an exercise. Since $(\sqrt{5} - 2)^{-1} = \sqrt{5} + 2$, we have

$$\sqrt{5} = [2; \overline{4}],$$

and so

$$\frac{p_{k+1}}{q_{k+1}} = 2 + \frac{1}{2 + \dfrac{p_k}{q_k}} = \frac{2p_k + 5q_k}{p_k + 2q_k}.$$

Since

$$\frac{2\mathrm{F}_2 + \mathrm{F}_3}{\mathrm{F}_3} = \frac{2+2}{2} = 2 = \frac{p_0}{q_0},$$

our claim holds when $n = 0$. If it holds when $n = k$ for some k, then

$$\begin{aligned}\frac{p_{k+1}}{q_{k+1}} &= \frac{2(2\mathrm{F}_{3k+2} + \mathrm{F}_{3k+3}) + 5\mathrm{F}_{3k+3}}{2\mathrm{F}_{3k+2} + \mathrm{F}_{3k+3} + 2\mathrm{F}_{3k+3}} \\ &= \frac{4\mathrm{F}_{3k+2} + 7\mathrm{F}_{3k+3}}{2\mathrm{F}_{3k+2} + 3\mathrm{F}_{3k+3}} = \frac{4\mathrm{F}_{3k+4} + 3\mathrm{F}_{3k+3}}{2\mathrm{F}_{3k+4} + \mathrm{F}_{3k+3}} \\ &= \frac{\mathrm{F}_{3k+4} + 3\mathrm{F}_{3k+5}}{\mathrm{F}_{3k+4} + \mathrm{F}_{3k+5}} = \frac{\mathrm{F}_{3k+6} + 2\mathrm{F}_{3k+5}}{\mathrm{F}_{3k+6}},\end{aligned}$$

so the claim holds when $n = k + 1$. □

17. April 22, 2008 (Tuesday)

Continued fractions

We can give alternative proofs of Theorems 22 and 23, avoiding the computations, by developing more of the theory of continued fractions. We assume now simply that

$$\boxed{d \text{ is a positive non-square,}}$$

as on page 29. We let $\sqrt{d}$ be the x in (2.2) and (2.4), which define a_n and ξ_n in terms of x, and we let p_n and q_n be as defined by (3.1), (3.2), and (3.4), so that, in particular, p_n/q_n is the convergent $[a_0; a_1, \ldots, a_n]$, by Theorem 1.

In case $d \in \{3, 14, 13\}$, as in (2.5), (8.2), and (8.3) on pages 22, 57, and 59, we have seen

$$\sqrt{d} = [a_0; \overline{a_1, \ldots, a_n}] \tag{17.1}$$

for some n. Now we shall show this generally, and, moreover, that (a, b) is a positive solution to the Pell equation (3.6) if and only if $(a, b) = (p_{n-1}, q_{n-1})$ for some *even* n such that $\sqrt{d} = [a_0; \overline{a_1, \ldots, a_n}]$. We already know part of this, implicitly, as follows.

Theorem 24. *Every positive solution of* (3.6) *is* (p_n, q_n) *for some* n.

Proof. Suppose (a, b) is such a solution. Note that a and b must be prime to one another. We have $a/b = p_n/q_n$ from

the proof of part (i) of Theorem 20, since this proof requires only that $\sqrt{d}$ be irrational. The equation of (a, b) and (p_n, q_n) follows, since p_n and q_n too are prime to one another, by Theorem 2. □

The computation of the continued-fraction expansions of particular $\sqrt{d}$ (as in the examples mentioned above) suggests the following.

Lemma 14. *There are sequences of rational integers s_n and t_n such that*

$$\xi_n = \frac{\sqrt{d} - t_n}{s_n}. \tag{17.2}$$

Proof. It is easy to establish that there are such rational *numbers* s_n and t_n. Indeed, this claim holds when $n = 0$, since $\xi_0 = \sqrt{d} - a_0$. Suppose for some k the claim holds when $n = k$. Then

$$\begin{aligned}\xi_{k+1} = \frac{1}{\xi_k} - a_{k+1} &= \frac{s_k}{\sqrt{d} - t_k} - a_{k+1} \\ &= \frac{\sqrt{d} + t_k}{\left(\dfrac{d - {t_k}^2}{s_k}\right)} - a_{k+1} = \frac{\sqrt{d} - \left(a_{k+1}\dfrac{d - {t_k}^2}{s_k} - t_k\right)}{\dfrac{d - {t_k}^2}{s_k}}.\end{aligned}$$

Thus the claim holds when $n = k + 1$. In particular,

$$s_{k+1} = \frac{d - {t_k}^2}{s_k}, \qquad t_{k+1} = a_{k+1}s_{k+1} - t_k. \tag{17.3}$$

We now show that s_n and t_n are integers. We have $s_0 = 1$ and $t_0 = a_0$. Then $s_1 = d - {a_0}^2$, an integer. Suppose s_k, t_k, and

s_{k+1} are integers. Immediately t_{k+1} is one too. Also,

$$s_{k+1} \mid d - {t_k}^2,$$
$$d - {t_{k+1}}^2 \equiv d - {t_k}^2 \equiv 0 \pmod{s_{k+1}},$$

and therefore s_{k+2} is an integer. □

The following needs only that $\sqrt{d}$ is irrational, so that the infinite expansion $[a_0; a_1, \dots]$ exists.

Lemma 15. *For all n,*

$$\sqrt{d} = [a_0; a_1, \dots, a_{n-1}, a_n + \xi_n].$$

Proof. The claim is trivially true when $n = 0$. Also, since $a_{k+1} + \xi_{k+1} = {\xi_k}^{-1}$ by (2.4), by (2.6) we have

$$[a_0; a_1, \dots, a_k, a_{k+1} + \xi_{k+1}] = [a_0; a_1, \dots, a_{k-1}, a_k + \xi_k]. \quad \square$$

Theorem 25. *If s_{n+1} is as in Lemma 14, then*

$${p_n}^2 - d{q_n}^2 = (-1)^{n+1} s_{n+1}.$$

Proof. In case $n = 0$, we have

$${p_0}^2 - d{q_0}^2 = {a_0}^2 - d = -s_1$$

as in the proof of Lemma 14. By (3.4), when $k \geqslant 1$, we have

$$\frac{p_{k+1}}{q_{k+1}} = \frac{p_k a_{k+1} + p_{k-1}}{q_k a_{k+1} + q_{k-1}}.$$

From this, by Lemma 15 we obtain

$$\sqrt{d} = \frac{p_k(a_{k+1} + \xi_{k+1}) + p_{k-1}}{q_k(a_{k+1} + \xi_{k+1}) + q_{k-1}}$$

or rather

$$(q_k a_{k+1} + q_{k-1})\sqrt{d} + q_k \xi_{k+1}\sqrt{d} = p_k a_{k+1} + p_{k-1} + p_k \xi_{k+1}.$$

By (17.2) this gives

$$\begin{aligned} s_{k+1}(q_k a_{k+1} + q_{k-1})\sqrt{d} + q_k(\sqrt{d} - t_{k+1})\sqrt{d} \\ = s_{k+1}(p_k a_{k+1} + p_{k-1}) + p_k(\sqrt{d} - t_{k+1}) \end{aligned}$$

and therefore

$$\begin{aligned} \big(s_{k+1}(q_k a_{k+1} + q_{k-1}) - q_k t_{k+1}\big)\sqrt{d} + q_k d \\ = \big(s_{k+1}(p_k a_{k+1} + p_{k-1}) - p_k t_{k+1}\big) + p_k\sqrt{d}. \end{aligned}$$

Since only $\sqrt{d}$ is irrational here, we obtain

$$\begin{cases} p_k = s_{k+1}(q_k a_{k+1} + q_{k-1}) - q_k t_{k+1}, \\ q_k d = s_{k+1}(p_k a_{k+1} + p_{k-1}) - p_k t_{k+1}. \end{cases}$$

Multiplying by p_k and q_k respectively, then subtracting, yields

$$p_k{}^2 - d q_k{}^2 = s_{k+1}(p_k q_{k-1} - q_k p_{k-1}) = (-1)^{k+1} s_{k+1}$$

by Theorem 2. □

Corollary. $s_n > 0$.

Proof. By Theorem 2 and its corollary,

$$\begin{aligned} (-1)^{n+1} = 1 \iff \frac{p_n}{q_n} > \sqrt{d} &\iff p_n - q_n\sqrt{d} > 0 \\ &\iff p_n{}^2 - d q_n{}^2 > 0. \end{aligned}$$ □

Lemma 16. $[a_0; a_1, \ldots, a_n]$ *determines* a_n.

Proof. The claim is easy when $0 \leqslant n \leqslant 1$. In the other cases, by Theorem 1,

$$\frac{p_{m+2}}{q_{m+2}} = \frac{p_{m+1}a_{m+2} + p_m}{q_{m+1}a_{m+2} + q_m},$$

and now we can solve for a_{m+2}. Indeed we obtain

$$a_{m+2}(p_{m+2}q_{m+1} - p_{m+1}q_{m+2}) = p_{m+2}q_m + p_m q_{m+2},$$

which yields a_{m+2} since $p_{m+2}/q_{m+2} \neq p_{m+1}/q_{m+1}$ by Theorem 2. □

Theorem 26. (17.1) *holds for some n. If m is the least such n, then the positive solutions of the Pell equation* (3.6) *are precisely (p_{km-1}, q_{km-1}), where $k > 0$ and km is even.*

Proof. The Pell equation has a positive solution by Lemma 2. This solution is (p_{n-1}, q_{n-1}) for some n, by Theorem 24. Since $s_n > 0$ by the corollary of Theorem 25, the theorem itself yields that $s_n = 1$ and n is even. Then $\xi_n = \sqrt{d} - t_n$ by Lemma 14, and t_n is unique such that $0 < \sqrt{d} - t_n < 1$. But $0 < \sqrt{d} - a_0 < 1$, so $t_n = a_0$, and $\xi_n = \xi_0$. Therefore $a_{n+1} = a_1$, and $\xi_{n+1} = \xi_1$, and so forth, so (17.1) holds. If m is the least such n, then, for any such n, we must have $m \mid n$.

Conversely, suppose $\sqrt{d} = [a_0; \overline{a_1, \ldots, a_m}]$. Then

$$\begin{aligned}\sqrt{d} &= [a_0; a_1, \ldots, a_{km-1}, a_{km}, \overline{a_1, \ldots, a_m}] \\ &= [a_0; a_1, \ldots, a_{km-1}, a_{km} - a_0 + a_0, \overline{a_1, \ldots, a_m}] \\ &= [a_0; a_1, \ldots, a_{km-1}, a_{km} - a_0 + \sqrt{d}].\end{aligned}$$

But also

$$\sqrt{d} = [a_0; a_1, \ldots, a_{km-1}, a_{km} + \xi_{km}],$$

by Lemma 15; hence, by Lemma 16, $\xi_{km} = \sqrt{d} - a_0$. In particular, $s_{km} = 1$, so (p_{km-1}, q_{km-1}) solves (3.6) by Theorem 25, as long as km is even. □

Porism. *If* (17.1) *holds, then* $\xi_{n+k} = \xi_k$ *for all* k.

Proof. Under the assumption, ${p_{n-1}}^2 - d{q_{n-1}}^2 = (-1)^n$, so $s_n = 1$, and $\xi_n = \xi_0$. Hence the claim. □

Some of the computations in Theorems 22 and 23 are special cases of the following.

Theorem 27. *If* $\sqrt{d} = [a_0; \overline{a_1, \ldots, a_n}]$, *then*

$$p_{k+n} + q_{k+n}\sqrt{d} = (p_{n-1} + q_{n-1}\sqrt{d})(p_k + q_k\sqrt{d}),$$

equivalently,

$$\begin{pmatrix} p_{k+n} \\ q_{k+n} \end{pmatrix} = \begin{pmatrix} p_{n-1} & dq_{n-1} \\ q_{n-1} & p_{n-1} \end{pmatrix} \begin{pmatrix} p_k \\ q_k \end{pmatrix}.$$

Proof. As in the proof of Theorem 26, we have

$$\begin{aligned} \sqrt{d} &= [a_0; a_1, \ldots, a_{n-1}, a_n - a_0 + a_0, \overline{a_1, \ldots, a_n}] \\ &= [a_0; a_1, \ldots, a_{n-1}, a_n - a_0 + \sqrt{d}]. \quad (17.4) \end{aligned}$$

By Theorem 1 then,

$$\begin{aligned} \sqrt{d} &= \frac{(a_n - a_0 + \sqrt{d})p_{n-1} + p_{n-2}}{(a_n - a_0 + \sqrt{d})q_{n-1} + q_{n-2}} \\ &= \frac{p_{n-1}\sqrt{d} + (a_n - a_0)p_{n-1} + p_{n-2}}{q_{n-1}\sqrt{d} + (a_n - a_0)q_{n-1} + q_{n-2}}. \quad (17.5) \end{aligned}$$

Here, if $n = 1$, then $p_{n-2} = 1$ and $q_{n-2} = 0$. Since $\sqrt{d}$ is irrational,

$$\begin{cases} dq_{n-1} = (a_n - a_0)p_{n-1} + p_{n-2}, \\ p_{n-1} = (a_n - a_0)q_{n-1} + q_{n-2}. \end{cases} \tag{17.6}$$

Putting these values into (17.5) and using (17.4) again, we have

$$[a_0; a_1, \ldots, a_{n-1}, a_n - a_0 + \sqrt{d}] = \frac{p_{n-1}\sqrt{d} + dq_{n-1}}{q_{n-1}\sqrt{d} + p_{n-1}}.$$

Moreover, the same is true if we put p_k/q_k in place of $\sqrt{d}$, leaving d itself unchanged since it comes from (17.6). Thus

$$\frac{p_{k+n}}{q_{k+n}} = \left[a_0; a_1, \ldots, a_{n-1}, a_n - a_0 + \frac{p_k}{q_k}\right] = \frac{p_{n-1}p_k + dq_{n-1}q_k}{q_{n-1}p_k + p_{n-1}q_k}.$$

We are done, once we establish that the last fraction is in lowest terms. We write it as a/b in the same terms. By Theorem 26 (strictly speaking, the proof),

$$p_{n-1}{}^2 - dq_{n-1}{}^2 = (-1)^n.$$

Using this, we compute

$$\begin{aligned} q_{n-1}a - p_{n-1}b &= -(-1)^n q_k, \\ p_{n-1}a - dq_{n-1}b &= (-1)^n p_k. \end{aligned}$$

Since $\gcd(p_k, q_k) = 1$, we must have $\gcd(a, b) = 1$. □

As a refinement of Theorem 26, we have the following.

Theorem 28. *For some n,*

$$\sqrt{d} = [a_0; \overline{a_1, \ldots, a_{n-1}, 2a_0}],$$

where, when $0 < k < n$,

$$a_k = a_{n-k} \tag{17.7}$$

Proof. By Theorem 26, (17.1) holds. We shall show first

$$\xi_k = \frac{1}{-\xi_{n-(k+1)}{}'} \tag{17.8}$$

whenever $0 \leqslant k < n$. By (17.3) in the proof of Lemma 14,

$$\frac{1}{\xi_k} = \frac{s_k}{\sqrt{d} - t_k} = \frac{\sqrt{d} + t_k}{s_{k+1}}.$$

Now using also Lemma 15, as well as (3.4) and Theorem 1, we have

$$\begin{aligned} & s_{k+1} \cdot \frac{1}{\xi_k} \\ & = \sqrt{d} + t_k = \left[a_0 + t_k; a_1, \ldots, a_k, \frac{1}{\xi_k}\right] = \frac{p_k \cdot \frac{1}{\xi_k} + p_{k-1}}{q_k \cdot \frac{1}{\xi_k} + q_{k-1}}, \end{aligned}$$

from which we obtain

$$s_{k+1}q_k \cdot \left(\frac{1}{\xi_k}\right)^2 + (s_{k+1}q_{k-1} - p_k) \cdot \frac{1}{\xi_k} - p_{k-1} = 0.$$

Let us write this as $f({\xi_k}^{-1}) = 0$. The coefficients of f being rational, also $1/{\xi_k}'$ is a zero of f. Moreover,

$$\begin{aligned} f(-1) = s_{k+1}(q_k - q_{k-1}) + p_k - p_{k-1} > 0, \\ f(0) = -p_{k-1} < 0, \end{aligned}$$

so f has a root between -1 and 0. That root must be $1/{\xi_k}'$, since $1/\xi_k > 0$. Thus

$$0 < \frac{1}{-\xi_k{}'} < 1.$$

We also have

$$0 < \xi_k < 1.$$

We can now establish (17.8) by induction. By the porism to Theorem 26, and because

$$\xi_0 = \sqrt{d} - a_0, \tag{17.9}$$

we obtain

$$\frac{1}{\xi_{n-1}} = a_n + \xi_n = \xi_0 + a_n = \sqrt{d} - a_0 + a_n$$

and therefore

$$\frac{1}{-\xi_{n-1}{}'} = \sqrt{d} + a_0 - a_n.$$

Comparing with (17.9), noting that both values are between 0 and 1, we obtain

$$\xi_0 = \frac{1}{-\xi_{n-1}{}'}, \qquad\qquad a_n = 2a_0.$$

In particular, we have (17.8) when $k = 0$. Suppose we have it when $k = j$, where $j + 1 < n$. Then

$$\begin{aligned}\xi_{j+1} + a_{j+1} = \frac{1}{\xi_j} = -\xi_{n-(j+1)}{}' &= -\Big(\frac{1}{\xi_{n-(j+2)}} - a_{n-(j+1)}\Big)' \\ &= -\frac{1}{\xi_{n-(j+2)}{}'} + a_{n-(j+1)}.\end{aligned}$$

As before, we must have (17.8) when $k = j + 1$. By induction, we have it for all k such that $0 \leqslant k < n$, and incidentally we have (17.7) when $0 < k < n$. □

18. April 29, 2008 (Tuesday)

Norm of a lattice

From Theorem 6 (page 37) and Exercise 12 (page 132), we know $\mathfrak{O}_K$ is a Euclidean domain when $d \in \{-1, -3\}$. However, when $d = -5$, then

$$3 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5}), \tag{18.1}$$

although each factor is irreducible. To prove the irreducibility, suppose for example

$$1 + \sqrt{-5} = \alpha\beta.$$

Then $\mathrm{N}(\alpha)\,\mathrm{N}(\beta) = \mathrm{N}(\alpha\beta) = \mathrm{N}\left(1 + \sqrt{-5}\right) = 6$. But no element of $\mathfrak{O}_K$ has norm 2, since the equation

$$x^2 + 5y^2 = 2$$

is insoluble. Hence one of $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$ is 1, so α or β is a unit. Thus there can be irreducibles that are not prime.

To avoid such problems, instead of working with the *numbers* in a quadratic field, we shall work with "ideal numbers," or what we now call simply *ideals*. Recall that an ideal of a commutative ring R is an additive subgroup of R that is closed under multiplication by elements of R. In other words, it is an R-submodule of R. (The definition of R-module is the same as the definition of a real vector-space, with $\mathbb{R}$ replaced by R.)

We shall generalize this definition slightly so that every lattice Λ of the quadratic field K will be an ideal of $\mathfrak{O}_\Lambda$, even if $\Lambda \not\subseteq \mathfrak{O}_\Lambda$. Let $\mathfrak{O}$ be an **order** of K, that is, a sub-ring of $\mathfrak{O}_K$ that spans K as a vector-space over $\mathbb{Q}$. Then $\mathfrak{O}$ is a lattice Λ by Lemma 6 (page 66), and $\mathfrak{O}_\Lambda = \mathfrak{O}$ by Exercise 26 (page 134). An additive subgroup G of K is an **ideal** of $\mathfrak{O}$ if it is closed under multiplication by elements of $\mathfrak{O}$, *and* $\alpha G \subseteq \mathfrak{O}$ for some non-zero α in K; we also require $G \neq \{0\}$.

Theorem 29. *Ideals of $\mathfrak{O}$ are lattices of K.*

Proof. Let L be an ideal of $\mathfrak{O}$. We have $\mathfrak{O} = \langle 1, c\omega \rangle$ for some positive rational integer c by Theorem 12 (page 68). Now use Lemma 6. There, (i) is immediate. For (ii), note that L contains some non-zero α, hence also $\alpha c\omega$. But $\{\alpha, \alpha c\omega\}$ is a basis of K over $\mathbb{Q}$. For (iii), we have $\beta L \subseteq \mathfrak{O}$ for some non-zero β. Multiplying β by some positive rational integer, we may assume $\beta \in \mathfrak{O}$. Then $\beta' \in \mathfrak{O}$, so $\mathrm{N}(\beta) L = \beta' \beta L \subseteq \beta' \mathfrak{O} \subseteq \mathfrak{O}$. □

So ideals are nothing new for us. Instead of saying that Λ is an ideal of $\mathfrak{O}_\Lambda$, we may say that Λ **belongs to** $\mathfrak{O}_\Lambda$.

Given an order, we aim to develop something like unique factorization for the lattices belonging to it. To do this, we define a **norm** for lattices.

In the original sense of norm, in any quadratic field K, if $n \in \mathbb{Z}$, then $\mathrm{N}(n) = n^2$. We want this to be the norm of the smallest ideal of $\mathfrak{O}_K$ that contains n. This ideal is $n\mathfrak{O}_K$ or $\langle n, n\omega \rangle$, and the quotient group $\mathfrak{O}_K / n\mathfrak{O}_K$ or $\langle 1, \omega \rangle / \langle n, n\omega \rangle$ has size n^2. Indeed, every coset of $\langle n, n\omega \rangle$ is $a + b\omega + \langle n, n\omega \rangle$

for some a and b in $\mathbb{Z}$, but

$$a + b\omega + \langle n, n\omega\rangle = s + t\omega + \langle n, n\omega\rangle \iff a \equiv s \ \ \& \ \ b \equiv t \bmod n,$$

so there are just n^2 distinct cosets. Generalizing this idea, we define

$$\mathrm{N}(\Lambda) = |\mathfrak{O}_\Lambda/\Lambda| = (\mathfrak{O}_\Lambda : \Lambda),$$

assuming $\Lambda \subseteq \mathfrak{O}_\Lambda$; in this case, Λ is an **integral** lattice.

Suppose Λ and M are arbitrary lattices of K, and $\Lambda \subseteq M$. What is $(M : \Lambda)$? We can write M as $\langle \alpha, \beta\rangle$; then

$$\Lambda = \langle e\alpha + f\beta, g\alpha + h\beta\rangle.$$

By the Euclidean algorithm, we can eliminate β from one generator. Indeed, suppose $\gcd(f, h) = a$, so that $fx + hy = a$ for some x and y in $\mathbb{Z}$. Then

$$\begin{vmatrix} h/a & -f/a \\ x & y \end{vmatrix} = 1,$$

$$\begin{pmatrix} h/a & -f/a \\ x & y \end{pmatrix} \begin{pmatrix} e\alpha + f\beta \\ g\alpha + h\beta \end{pmatrix} = \begin{pmatrix} (he - fg)\alpha/a \\ (ex + gy)\alpha + a\beta \end{pmatrix}.$$

Thus

$$\Lambda = \langle b\alpha, c\alpha + a\beta\rangle, \tag{18.2}$$

where $b = (he - fg)/a$ and $c = ex + gy$. In particular,

$$|ab| = \left|\det \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right|. \tag{18.3}$$

We may then assume that $b > 0$ and $0 \leqslant c < b$, while (18.2) and (18.3) continue to hold. Then the cosets of Λ in M are

in one-to-one correspondence with the pairs (i, j) such that $0 \leqslant i < a$ and $0 \leqslant j < b$. That is, every element of M is congruent *modulo* Λ to some unique $j\alpha + i\beta$, where $0 \leqslant i < a$ and $0 \leqslant j < b$. Thus

$$(M : \Lambda) = ab = \left|\det \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right| = \sqrt{\begin{vmatrix} e & f \\ g & h \end{vmatrix}^2}.$$

For example, if $M = \langle 1, \mathrm{i} \rangle$ and $\Lambda = \langle 3, 1 + 2\,\mathrm{i} \rangle$, then $(M : \Lambda) = |M/\Lambda| = 6$; equivalently, every element of M is congruent *modulo* Λ to one of the six elements lying within the parallelogram depicted in Figure 18.1. In the general situa-

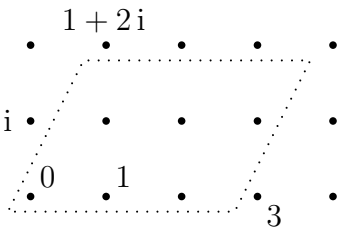

Figure 18.1.: Lattices $\langle 1, \mathrm{i} \rangle$ and $\langle 3, 1 + 2\,\mathrm{i} \rangle$

tion, recalling the discriminant of a lattice as defined in (9.4) on page 64, we have

$$(M : \Lambda)^2 = \begin{vmatrix} e & f \\ g & h \end{vmatrix}^2 = \frac{\begin{vmatrix} e & f \\ g & h \end{vmatrix}^2 \begin{vmatrix} \alpha & \alpha' \\ \beta & \beta' \end{vmatrix}^2}{\begin{vmatrix} \alpha & \alpha' \\ \beta & \beta' \end{vmatrix}^2} = \frac{\Delta(\Lambda)}{\Delta(M)}.$$

We can use this to define the norm in general:

$$\mathrm{N}\,(\Lambda) = \sqrt{\frac{\Delta(\Lambda)}{\Delta(\mathfrak{O}_\Lambda)}}.$$

This is always positive, unlike the norm of some numbers when $d > 0$. But suppose $\alpha \in K$, and let $\mathfrak{O}$ be an order of K. Then $\alpha\mathfrak{O}$ is a lattice belonging to $\mathfrak{O}$; and since $\mathfrak{O} = \langle 1, c\omega \rangle$ for some positive rational integer c, we have

$$\mathrm{N}\,(\alpha\mathfrak{O}) = \sqrt{\frac{\begin{vmatrix} \alpha & \alpha' \\ \alpha c\omega & \alpha' c\omega' \end{vmatrix}^2}{\begin{vmatrix} 1 & 1 \\ c\omega & c\omega' \end{vmatrix}^2}} = \sqrt{(\alpha\alpha')^2} = |\mathrm{N}\,(\alpha)|.$$

19. May 2, 2008 (Friday)

Products of lattices

The product of lattices Λ and M of K is the smallest subgroup of K that includes the set $\{xy : x \in \Lambda \quad \& \quad y \in M\}$. If $\Lambda = \langle \alpha, \beta \rangle$ and $M = \langle \gamma, \delta \rangle$, then

$$\Lambda M = \langle \alpha\gamma, \alpha\delta, \beta\gamma, \beta\delta \rangle.$$

Then ΛM is a lattice by Lemma 6, since $\mathfrak{O}_K$ includes $m\Lambda$ and nM, and therefore $nm\Lambda M$, for some m and n, and ΛM spans K since ΛM contains $\alpha\gamma$ and $\beta\gamma$, which span.

Lemma 17. *Multiplication of lattices is commutative and associative, and*

$$\mathfrak{O}_\Lambda \cdot \Lambda = \Lambda.$$

Proof. The first part follows from the same properties of multiplication of numbers. For the second part, $\Lambda \subseteq \mathfrak{O}_\Lambda \cdot \Lambda$ since $1 \in \mathfrak{O}_\Lambda$, and $\mathfrak{O}_\Lambda \cdot \Lambda \subseteq \Lambda$ by definition of $\mathfrak{O}_\Lambda$. □

Lemma 18. *For all lattices Λ belonging to an order $\mathfrak{O}$,*

$$\Lambda\Lambda' = \mathrm{N}(\Lambda) \cdot \mathfrak{O}.$$

Proof. Suppose first $\Lambda = \langle 1, \tau \rangle$, where

$$A\tau^2 + B\tau + C = 0, \qquad \gcd(A, B, C) = 1, \qquad A > 0.$$

Then

$$\frac{B}{A} = -(\tau + \tau'), \qquad \frac{C}{A} = \tau\tau', \qquad \mathfrak{O}_\Lambda = \langle 1, A\tau \rangle.$$

Hence

$$\begin{aligned}\langle 1, \tau\rangle\langle 1, \tau'\rangle = \langle 1, \tau', \tau, \tau\tau'\rangle &= \left\langle \frac{A}{A}, \tau, \frac{B}{A}, \frac{C}{A} \right\rangle \\ &= \left\langle \frac{1}{A}, \tau \right\rangle = \frac{1}{A}\langle 1, A\tau\rangle = \frac{1}{A} \cdot \mathfrak{O}_\Lambda.\end{aligned}$$

But

$$\mathrm{N}\left(\langle 1, \tau\rangle\right) = \sqrt{\frac{\begin{vmatrix} 1 & 1 \\ \tau & \tau' \end{vmatrix}^2}{\begin{vmatrix} 1 & 1 \\ A\tau & A\tau' \end{vmatrix}^2}} = \frac{1}{A}.$$

We can write an arbitrary lattice as $\langle \alpha, \alpha\tau \rangle$. Then

$$\begin{aligned}\langle \alpha, \alpha\tau\rangle\langle \alpha', \alpha'\tau'\rangle = \alpha\langle 1, \tau\rangle\alpha'\langle 1, \tau'\rangle = \alpha\alpha' \,\mathrm{N}\left(\langle 1, \tau\rangle\right) \mathfrak{O}_\Lambda \\ = \mathrm{N}\left(\langle \alpha, \alpha\tau\rangle\right) \mathfrak{O}_\Lambda,\end{aligned}$$

where Λ can be understood indifferently as $\langle 1, \tau\rangle$ or $\langle \alpha, \alpha\tau\rangle$, by Theorem 13. □

Theorem 30. *The lattices belonging to an order $\mathfrak{O}$ compose an abelian group under multiplication; the identity is $\mathfrak{O}$ itself, and inversion given by*

$$\Lambda^{-1} = \frac{1}{\mathrm{N}\left(\Lambda\right)}\Lambda'.$$

Proof. By Lemmas 17 and 18, it remains to show that the set of lattices belonging to $\mathfrak{O}$ is actually closed under multiplication. We compute

$$\begin{aligned} \mathrm{N}(\Lambda)\,\mathrm{N}(M)\cdot\mathfrak{O} &= \mathrm{N}(\Lambda)\cdot\mathfrak{O}\cdot\mathrm{N}(M)\cdot\mathfrak{O} \\ &= \Lambda\Lambda' MM' = (\Lambda M)(\Lambda M)' = \mathrm{N}(\Lambda M)\cdot\mathfrak{O}_{\Lambda M}. \end{aligned} \quad (19.1)$$

Since $\mathfrak{O} = \langle 1, c\omega\rangle$ and $\mathfrak{O}_{\Lambda M} = \langle 1, e\omega\rangle$ for some positive rational integers c and e, using the new expressions in (19.1) gives us

$$\mathrm{N}(\Lambda)\,\mathrm{N}(M) = \mathrm{N}(\Lambda M), \quad \mathrm{N}(\Lambda)\,\mathrm{N}(M)\,c\omega = \mathrm{N}(\Lambda M)\,e\omega,$$

and therefore $c = e$, so $\mathfrak{O}_{\Lambda M} = \mathfrak{O}$. □

Porism. *If Λ and M belong to the same order, then*

$$\mathrm{N}(\Lambda M) = \mathrm{N}(\Lambda)\,\mathrm{N}(M).$$

20. May 6, 2008 (Tuesday)

Arithmetic of lattices

In addition to multiplying, we can add lattices:

$$\Lambda + M = \{\xi + \eta \colon \xi \in \Lambda \ \ \& \ \ \eta \in M\}.$$

Proving the following is Exercise 27.

Lemma 19. *Let Λ and M be lattices of K.*

(i) *$\Lambda + M$ is a lattice, and*

$$\langle \alpha, \beta \rangle + \langle \gamma, \delta \rangle = \langle \alpha, \beta, \gamma, \delta \rangle.$$

(ii) *Addition of lattices is commutative and associative.*

(iii) *Multiplication of lattices distributes over addition.*

(iv) *If Λ and M belong to $\mathfrak{O}$, then $\mathfrak{O} \subseteq \mathfrak{O}_{\Lambda+M}$.*

(v) *If Λ and M belong to $\mathfrak{O}_K$, then $\mathfrak{O}_{\Lambda+M} = \mathfrak{O}_K$.*

Although Λ and M belong to the same order $\mathfrak{O}$, possibly $\Lambda + M$ does not belong to $\mathfrak{O}$. For example, $\langle n, 1 + \omega \rangle$ and $\langle 1, n\omega \rangle$ both belong to $\langle 1, n\omega \rangle$ (Exercise 28), but

$$\langle n, 1 + \omega \rangle + \langle 1, n\omega \rangle = \langle n, 1 + \omega, 1, n\omega \rangle = \langle 1, \omega \rangle.$$

We aim to show that the integral lattices belonging to $\mathfrak{O}$ have unique prime factorizations. What does this mean? The integral lattices have norms that are positive rational integers, since in this case $\mathrm{N}(\Lambda) = (\mathfrak{O} : \Lambda)$. Also,

$$\mathrm{N}(\Lambda) = 1 \iff \Lambda = \mathfrak{O}$$

(again assuming $\Lambda \subseteq \mathfrak{O}$). By the porism to Theorem 30, no non-trivial factorization can go on forever. That is, we obtain

$$\Lambda = P_1 P_2 \cdots P_n, \tag{20.1}$$

where each P_i is an integral lattice of norm greater than 1, with no factors other than itself and $\mathfrak{O}$. In a word, each P_i is **irreducible.**

For example, if $\mathrm{N}(P)$ is a rational prime p, then P is irreducible, since p is irreducible:

$$\begin{aligned} P = \Lambda_0 \Lambda_1 &\implies p = \mathrm{N}(P) = \mathrm{N}(\Lambda_0)\,\mathrm{N}(\Lambda_1) \\ &\implies \mathrm{N}(\Lambda_i) = 1 \text{ for some } i \\ &\implies \Lambda_i = \mathfrak{O} \ \ \& \ \ \Lambda_{1-i} = P \text{ for some } i. \end{aligned}$$

We want (if possible) to establish uniqueness of the factorization in (20.1). For this, we use the notion of a **prime** lattice. Working with the integral lattices of some order $\mathfrak{O}$, we define **divisibility** by

$$\Lambda \mid M \iff \Lambda A = M \text{ for some } A.$$

Theorem 31. *For all integral lattices Λ and M of an order $\mathfrak{O}$,*

$$\Lambda \mid M \iff M \subseteq \Lambda.$$

Proof. If $\Lambda A = M$, where $A \subseteq \mathfrak{O}$, then $M = \Lambda A \subseteq \Lambda\mathfrak{O} = \Lambda$. Conversely, suppose $M \subseteq \Lambda$. Then

$$\Lambda \cdot \frac{1}{\mathrm{N}(\Lambda)} \Lambda' M = \mathfrak{O} M = M, \qquad \frac{1}{\mathrm{N}(\Lambda)} \Lambda' M \subseteq \frac{1}{\mathrm{N}(\Lambda)} \Lambda' \Lambda = \mathfrak{O},$$

so $(1/\mathrm{N}(\Lambda))\Lambda' M$ is integral, and hence $\Lambda \mid M$. □

Having division, we may have *greatest common divisors:* An integral lattice Π is a **greatest common divisor** of Λ and M, provided

$$\Pi \mid \Lambda \ \& \ \Pi \mid M,$$
$$\Sigma \mid \Lambda \ \& \ \Sigma \mid M \implies \Sigma \mid \Pi.$$

But what *is* Π here? We have

$$\Lambda, M \subseteq \Lambda + M;$$
$$\Lambda, M \subseteq \Sigma \implies \Lambda + M \subseteq \Sigma.$$

Since $\Lambda + M \subseteq \mathfrak{O}$, we can apply Theorem 31, *provided* $\Lambda + M$ also belongs to $\mathfrak{O}$. We have this in case $\mathfrak{O}$ is $\mathfrak{O}_\Lambda$, by Lemma 19 (v):

Lemma 20. *The sum of integral lattices of $\mathfrak{O}_K$ is their greatest common divisor.*

An integral lattice P is **prime** if

$$P \mid \Lambda M \ \& \ P \nmid \Lambda \implies P \mid M,$$

equivalently,

$$\Lambda M \subseteq P \ \& \ \Lambda \not\subseteq P \implies M \subseteq P.$$

Lemma 21. *Irreducible integral lattices of $\mathfrak{O}_K$ are prime.*

Proof. Suppose Π is irreducible, and $\Lambda M \subseteq \Pi$, but $\Lambda \not\subseteq \Pi$. Sincet $\Pi + \Lambda \mid \Pi$ by Lemma 20, and Π is irreducible, $\Pi + \Lambda$ is either Π or $\mathfrak{O}$. But $\Pi \nmid \Lambda$, so $\Pi + \Lambda = \mathfrak{O}$. Hence

$$M = \mathfrak{O}M = (\Pi + \Lambda)M = \Pi M + \Lambda M.$$

But $\Lambda M = \Pi\Sigma$ for some integral Σ since $\Pi \mid \Lambda M$. Hence

$$M = \Pi M + \Pi\Sigma = \Pi(M + \Sigma).$$

By Lemma 19 (v), we have $\Pi \mid M$. □

Theorem 32. *The integral lattices of $\mathfrak{O}_K$ admit unique prime factorizations.*

Proof. The proof is as for the Fundamental Theorem of Arithmetic. Suppose $P_1P_2\cdots P_m$ and $Q_1Q_2\cdots Q_m$ are two irreducible factorizations of the same lattice Λ. Then $P_1 \mid \Lambda$, so $P_1 \mid Q_i$ for some i by Lemma 21. We may assume $i = 1$. Then $P_1 = Q_1$, since $P_1 \neq \mathfrak{O}_K$ and Q_1 is irreducible. We now have

$$P_1P_2\cdots P_m = P_1Q_2\cdots Q_n,$$
$$P_2\cdots P_m = Q_2\cdots Q_n$$

since we are in a group. Continuing, we get that $m = n$ and we may assume $P_i = Q_i$. □

21. May 9, 2008 (Friday)

Prime factorizations

We want to *find* prime factorizations. For example, letting $d = -5$ and $\mathfrak{O} = \mathfrak{O}_K$, so that this is $\langle 1, \omega \rangle$, from (18.1) we have, as an equation of products of integral lattices of $\mathfrak{O}$,

$$(3\mathfrak{O})(2\mathfrak{O}) = ((1+\omega)\mathfrak{O})((1-\omega)\mathfrak{O}). \tag{21.1}$$

Since

$$(1 \pm \omega)\mathfrak{O} = \langle 1 \pm \omega, \omega \pm \omega^2 \rangle = \langle 1 \pm \omega, \omega \mp 5 \rangle = \langle 1 \pm \omega, 6 \rangle,$$

we can write (21.1) as

$$\langle 3, 3\omega \rangle \langle 2, 2\omega \rangle = \langle 6, 1+\omega \rangle \langle 6, 1-\omega \rangle.$$

By Theorem 32, the factors here cannot be prime. What then are the prime factors of, for example, $2\mathfrak{O}$, which is $\langle 2, 2\omega \rangle$? We have $\mathrm{N}(2\mathfrak{O}) = \mathrm{N}(2)\,\mathrm{N}(\mathfrak{O}) = 4$, so we should look for factors of norm 2. Two possibilities are $\langle 2, \omega \rangle$ and $\langle 1, 2\omega \rangle$. But

$$\langle 2, \omega \rangle = 2\Big\langle 1, \frac{1}{2}\omega \Big\rangle, \qquad\qquad 4\left(\frac{1}{2}\omega\right)^2 + 5 = 0,$$

and therefore, by Theorems 13 and 14 (page 69),

$$\mathfrak{O}_{\langle 2,\omega \rangle} = \Big\langle 1, 4 \cdot \frac{1}{2}\omega \Big\rangle = \langle 1, 2\omega \rangle,$$

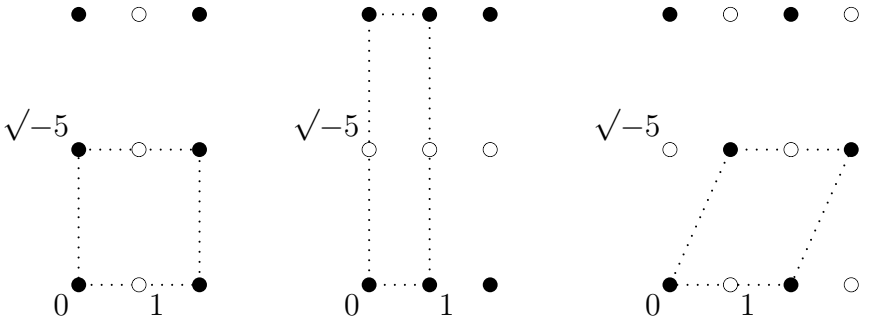

Figure 21.1.: Index-2 sublattices of $\langle 1, \sqrt{-5}\rangle$

which is not $\mathfrak{O}$. In particular, $\langle 2, \omega\rangle$ does not belong to $\mathfrak{O}$. Similarly, $\langle 1, 2\omega\rangle$ does not, but belongs to itself.

A third option for a prime factor of $\langle 2, 2\omega\rangle$ is $\langle 2, 1+\omega\rangle$. (See Figure 21.1.) This works: if $\alpha = (1+\omega)/2$, then

$$(2\alpha - 1)^2 = -5, \qquad 4\alpha^2 - 4\alpha + 6 = 0,$$

so $2\alpha^2 - 2\alpha + 3 = 0$, and $\langle 2, 1+\omega\rangle$ belongs to $\mathfrak{O}$. Moreover $\langle 2, 1+\omega\rangle' = \langle 2, 1+\omega\rangle$, so by Lemma 18,

$$\langle 2, 1+\omega\rangle^2 = 2\mathfrak{O}.$$

Now let d be arbitrary, $\mathfrak{O} = \mathfrak{O}_K$, and P be a prime lattice of $\mathfrak{O}$. There is a non-zero element α of P. Then $\alpha' \in \mathfrak{O}$, so P contains $\alpha\alpha'$, a rational integer. Since P is prime, the least positive rational integer that it contains must be prime. Suppose this is p. then

$$P \mid p\mathfrak{O}.$$

Conversely, suppose p is a rational prime, and P is a prime factor of $p\mathfrak{O}$. Then

$$\mathrm{N}\,(P) \mid p^2.$$

- If $\mathrm{N}(P) = p^2$, this means P is just $p\mathfrak{O}$.
- If $\mathrm{N}(P) = p$, then $PP' = p\mathfrak{O}$, but possibly $P = P'$.

So there are three possibilities.

(i) If $p\mathfrak{O}$ is itself prime, then p is **inert** in $\mathfrak{O}$;

(ii) If $p\mathfrak{O} = PP'$, where $P \neq P'$, then p **splits** in $\mathfrak{O}$;

(iii) If $p\mathfrak{O} = P^2$, then p **ramifies** in $\mathfrak{O}$.

22. May 20, 2008 (Tuesday)

Primes

To compute which of the three possibilities actually happens, it is convenient to let

$$\Delta = \Delta(\mathfrak{O}) = \begin{vmatrix} 1 & 1 \\ \omega & \omega' \end{vmatrix}^2 = \begin{cases} d, & \text{if } d \equiv 1 \pmod 4; \\ 4d, & \text{if } d \not\equiv 1. \end{cases}$$

Theorem 33.

(i) *If $p \nmid \Delta$, and $\Delta \equiv x^2 \pmod{4p}$ has no solution, then p is inert in $\mathfrak{O}$.*

(ii) *If $p \nmid \Delta$, and $\Delta \equiv s^2 \pmod{4p}$, then p splits in $\mathfrak{O}$, and*

$$p\mathfrak{O} = \left\langle p, \frac{s + \sqrt{\Delta}}{2} \right\rangle \left\langle p, \frac{s - \sqrt{\Delta}}{2} \right\rangle.$$

(iii) *If $p \mid \Delta$, then p ramifies in $\mathfrak{O}$, and*

$$p\mathfrak{O} = \begin{cases} \left\langle p, \dfrac{\Delta + \sqrt{\Delta}}{2} \right\rangle^2, & \text{if } p \text{ is odd;} \\ \langle 2, \sqrt{d} \rangle^2, & \text{if } p = 2 \ \ \& \ \ d \equiv 2; \\ \langle 2, 1 + \sqrt{d} \rangle^2, & \text{if } p = 2 \ \ \& \ \ d \equiv 3. \end{cases}$$

Proof. Suppose p is not inert in $\mathfrak{O}$. Then $p\mathfrak{O}$ has a proper prime factor P, of norm p, so that

$$(\mathfrak{O} : P) = p.$$

So there are just p distinct congruence-classes *modulo* P. Moreover, they are represented by the elements of $\{0, 1, \ldots, p-1\}$. Indeed, if $0 \leqslant i \leqslant j < p$, and $i \equiv j \pmod{P}$, then $P \mid (j-i)\mathfrak{O}$, so $\mathrm{N}(P) \mid \mathrm{N}((j-i)\mathfrak{O})$, that is,

$$p \mid (j-i)^2,$$

so $i = j$. Therefore, in particular, there is a rational integer r such that $0 \leqslant r < p$ and

$$\begin{gathered}
\frac{\Delta + \sqrt{\Delta}}{2} \equiv r \pmod{P}, \\
2r - \Delta - \sqrt{\Delta} \equiv 0 \pmod{2P}, \\
2P \mid (2r - \Delta - \sqrt{\Delta})\mathfrak{O}, \\
\mathrm{N}(2P) \mid \mathrm{N}\left((2r - \Delta - \sqrt{\Delta})\mathfrak{O}\right), \\
4p \mid (2r - \Delta)^2 - \Delta, \\
\Delta \equiv (2r - \Delta)^2 \pmod{4p}.
\end{gathered}$$

This proves (i).

Now suppose $\Delta \equiv s^2 \pmod{4p}$, and let

$$P = \left\langle p, \frac{s + \sqrt{\Delta}}{2} \right\rangle.$$

To compute $\mathfrak{O}_P$ by means of Theorem 14, we have

$$\begin{aligned}
\alpha = \frac{s + \sqrt{\Delta}}{2p} &\implies 2p\alpha - s = \sqrt{\Delta} \\
&\implies 4p^2\alpha^2 - 4ps\alpha + s^2 - \Delta = 0 \\
&\implies p\alpha^2 - s\alpha + \frac{s^2 - \Delta}{4p} = 0.
\end{aligned}$$

If $p \nmid \Delta$, then $p \nmid s$, and we can conclude

$$\mathfrak{O}_P = \left\langle 1, \frac{s + \sqrt{\Delta}}{2} \right\rangle = \mathfrak{O}.$$

So P belongs to $\mathfrak{O}$; and it has norm p, so $p\mathfrak{O} = PP'$ by Lemma 18. Finally, $P \neq P'$, since $P + P'$ contains s, but P does not. Thus (ii).

Finally, to prove (iii), since each of the given lattices is its own conjugate, it is enough to show that the lattices belong to $\mathfrak{O}$. For example, in case p is odd, assuming $p \mid \Delta$, we have

$$\begin{aligned} \alpha = \frac{\Delta + \sqrt{\Delta}}{2p} &\implies 2p\alpha - \Delta = \sqrt{\Delta} \\ &\implies 4p^2\alpha^2 - 4p\Delta\alpha + \Delta^2 - \Delta = 0 \\ &\implies p\alpha^2 - \Delta\alpha + \frac{\Delta^2 - \Delta}{4p} = 0. \end{aligned}$$

We always have $\Delta \equiv 0$ or $1 \pmod 4$, so $4 \mid \Delta^2 - \Delta$; hence $4p \mid \Delta^2 - \Delta$. But $\Delta^2 - \Delta = \Delta(\Delta - 1)$, and $p \nmid \Delta - 1$, but also $p^2 \nmid \Delta$, since d is square-free. Therefore $\langle p, (\Delta + \sqrt{\Delta})/2 \rangle$ does belong to $\mathfrak{O}$. The remaining cases are easier. □

For example, if $d = 21$, then $\Delta = 21$, and the primes ramifying in $\mathfrak{O}$ are just 3 and 7.

A. Exercises

A.1. February 26, 2008

Exercise 1. Let S be the set of Pythagorean triples (a, b, c) such that $\gcd(a, b, c) = 1$; a, b, and c are positive; and $a < b$. Order S by the rule

$$(a, b, c) < (d, e, f) \iff (a+b < d+e) \text{ or } (a+b = d+e \wedge b < e).$$

Find the first few elements of S with respect to this ordering.

Exercise 2. Solve $x^2 + 4y^2 = z^2$.

Exercise 3. Solve $x^4 + y^2 = z^2$.

Exercise 4. (i) Show that $f(x, y) = 0$ is soluble if and only if $f(3x + 2y, 4x + 3y) = 0$ is soluble.

(ii) Find necessary and sufficient conditions on a, b, c, and d such that an arbitrary Diophantine equation $f(x, y) = 0$ is soluble if and only if $f(ax+by, cx+dy) = 0$ is soluble.

Exercise 5. (i) Find the expansion of $\sqrt{d}$ as a continued fraction for various d, including 7.

(ii) Solve the Pell equation $x^2 - dy^2 = 1$ for these d.

Exercise 6. (i) Show $[a_0; a_1, \ldots, a_k, a_{k+1}, \ldots, a_n] =$

$$[a_0; a_1, \ldots, a_k, [a_{k+1}, \ldots, a_n]].$$

(ii) Show $[a_0; a_1, \ldots, a_k, a_{k+1}, \ldots] =$

$$[a_0; a_1, \ldots, a_k, [a_{k+1}, \ldots]].$$

(iii) Compute $[\overline{2; 1}]$ (which is $[2; 1, \overline{2, 1}]$) in terms of radicals.

(iv) Show that $[a_0; a_1, \ldots, a_k, \overline{a_{k+1}, \ldots, a_n}]$ is always the root of a quadratic polynomial.

A.2. March 11, 2008

Exercise 7. If d is a positive non-square rational integer, prove $\sqrt{d}$ is irrational.

Exercise 8. Find a greatest common divisor α of the Gaussian integers $27 + 55\,\mathrm{i}$ and $20 + 18\,\mathrm{i}$, and solve

$$(27 + 55\,\mathrm{i})\xi + (20 + 18\,\mathrm{i})\eta = \alpha.$$

Exercise 9. Find all solutions of the Diophantine equation

$$x^2 + y^2 = 1170.$$

Exercise 10. Assuming n is positive, prove that the number of solutions of the Diophantine equation

$$x^2 + y^2 = n$$

is 4 times the excess of the number of positive factors of n that are congruent to 1 *modulo* 4 over the number that are congruent to 3 *modulo* 4.

Exercise 11. (i) Characterize (by describing their prime factorizations) those Gaussian integers α such that $|\alpha|^2$ is square as a rational integer.

(ii) Use this characterization to solve the Diophantine equation

$$x^2 + y^2 = z^2.$$

Exercise 12. The polynomial $x^2 + x + 1$ has two conjugate roots. Let ω be the root with positive imaginary part.

(i) Write ω in radicals.

(ii) Sketch $\mathbb{Z}[\omega]$ as a subset of the complex plane.

(iii) Letting $\mathrm{N}(z) = |z|^2$, show that $\mathrm{N}(\alpha) \in \mathbb{N}$ when $\alpha \in \mathbb{Z}[\omega]$.

(iv) Express $\mathrm{N}(x + \omega y)$ in terms of x and y.

(v) Show that $\mathbb{Z}[\omega]$ with $z \mapsto \mathrm{N}(z)$ is a Euclidean domain.

(The elements of $\mathbb{Z}[\omega]$ are the **Eisenstein integers.**)

A.3. April 3, 2008

Exercise 13. Verify that the integers of a quadratic field do compose a ring.

Exercise 14. Suppose $\tau = (15 + 3\sqrt{17})/4$. Find A, B, and C in $\mathbb{Z}$ such that $A\tau^2 + B\tau + C = 0$ and $\gcd(A, B, C) = 1$.

Exercise 15. Suppose $A\tau^2 + B\tau + C = 0$ for some A, B, and C in $\mathbb{Z}$, where $A > 0$ and $\gcd(A, B, C) = 1$.

(i) Show $\langle 1, A\bar{\tau}\rangle\langle 1, \tau\rangle = \langle 1, \tau\rangle$.

(ii) Show $\langle A, A\bar{\tau}\rangle\langle 1, \tau\rangle = \langle 1, A\bar{\tau}\rangle$.

(iii) Using (i) and (ii), show $\mathfrak{O}_\Lambda = \langle 1, A\bar{\tau}\rangle$, where $\Lambda = \langle 1, \tau\rangle$.

Exercise 16. Let Λ be the lattice

$$\left\langle \frac{3+5\sqrt{6}}{2}, \frac{6+\sqrt{6}}{3} \right\rangle$$

of $\mathbb{Q}(\sqrt{6})$. Find $\mathfrak{O}_\Lambda$.

Exercise 17. Suppose $\tau \in \mathbb{C} \smallsetminus \mathbb{Q}$. Show that the following are equivalent:

(i) $A\tau^2 + B\tau + C = 0$ for some A, B, and C in $\mathbb{Z}$;

(ii) $\alpha\langle 1, \tau\rangle \subseteq \langle 1, \tau\rangle$ for some α in $\mathbb{C} \smallsetminus \mathbb{Z}$.

Exercise 18. Let $f(x, y)$ be the quadratic form

$$60x^2 + 224xy - 735y^2.$$

(i) Find the discriminant of f in the form $n\sqrt{d}$, where n and d are rational integers, and d is square-free.

(ii) Find all solutions from $\mathbb{Z}$ of $f(x, y) = 1$.

(iii) Find all solutions from $\mathbb{Z}$ of $f(x, y) = 6$.

Exercise 19. For every lattice Λ of a quadratic field K, show that the units of $\mathfrak{O}_\Lambda$ are just the units of $\mathfrak{O}_K$ that are in $\mathfrak{O}_\Lambda$.

A.4. April 10, 2008

These exercises involve quadratic Diophantine equations.

Exercise 20. Solve

$$2x^2 + 2xy + y^2 = 25.$$

Exercise 21. Solve

$$9x^2 + 6xy + 2y^2 = 17.$$

Exercise 22. Solve (if you can!)

$$121x^2 + 304xy + 191y^2 = 37.$$

(If nothing else works, try letting $3x+4y = u$ and $4x+5y = v$.)

Exercise 23. Solve

$$4x^2 + 2xy - y^2 = 44.$$

Exercise 24. Concerning

$$8x^2 + 4xy - y^2 = m :$$

(i) solve when $m = 8$;

(ii) solve when $m = 44$;

(iii) find all m for which the equation is soluble, where $0 < m < 44$.

A.5. May 18, 2008

Exercise 25. Prove that the nth convergent of $\sqrt{5}$ is

$$\frac{2\mathrm{F}_{3n+2} + \mathrm{F}_{3n+3}}{\mathrm{F}_{3n+3}}.$$

Exercise 26. Verify that an order $\mathfrak{O}$ of K is in particular a lattice Λ such that $\mathfrak{O}_\Lambda = \mathfrak{O}$.

Exercise 27. Let Λ and M be lattices of K. Prove the following [which is Lemma 19].

(i) $\Lambda + M$ is a lattice, and

$$\langle \alpha, \beta \rangle + \langle \gamma, \delta \rangle = \langle \alpha, \beta, \gamma, \delta \rangle.$$

(ii) Addition of lattices is commutative and associative.

(iii) Multiplication of lattices distributes over addition.

(iv) If Λ and M belong to $\mathfrak{O}$, then $\mathfrak{O} \subseteq \mathfrak{O}_{\Lambda+M}$.

(v) If Λ and M belong to $\mathfrak{O}_K$, then $\mathfrak{O}_{\Lambda+M} = \mathfrak{O}_K$.

Exercise 28. Show that $\langle n, 1+\omega \rangle$ and $\langle 1, n\omega \rangle$ both belong to $\langle 1, n\omega \rangle$.

B. Examinations

B.1. March 24, 2008 (Monday)

Instructions. Take at most 90 minutes to write reasonably legible solutions on the blank sheets provided. You may want to do scratch-work first, on sheets that you will keep. But the sheets that you turn in should show sufficient work to justify your answers. You may keep this problem-sheet for future study. *Kolay gelsin.*

Problem 1. This problem involves the Gaussian integers. Let $\alpha = 40 + 5\,\mathrm{i}$ and $\beta = 39\,\mathrm{i}$.

(i) Find a greatest common divisor of α and β.

(ii) If γ is your answer to (i), solve

$$(40 + 5\,\mathrm{i}\,) \cdot \xi + 39\,\mathrm{i} \cdot \eta = \gamma.$$

Solution. (i) Apply the Euclidean algorithm:

$$\frac{\alpha}{\beta} = \frac{40 + 5\,\mathrm{i}}{39\,\mathrm{i}} = \frac{5 - 40\,\mathrm{i}}{39} = -\,\mathrm{i} + \frac{5 - \mathrm{i}}{39},$$
$$40 + 5\,\mathrm{i} = (39\,\mathrm{i})(-\,\mathrm{i}\,) + 1 + 5\,\mathrm{i};$$
$$\frac{39\,\mathrm{i}}{1 + 5\,\mathrm{i}} = \frac{195 + 39\,\mathrm{i}}{26} = 7 + \mathrm{i} + \frac{1 + \mathrm{i}}{2},$$
$$39\,\mathrm{i} = (1 + 5\,\mathrm{i}\,)(7 + \mathrm{i}\,) - 2 + 3\,\mathrm{i};$$
$$\frac{1 + 5\,\mathrm{i}}{-2 + 3\,\mathrm{i}} = \frac{(1 + 5\,\mathrm{i}\,)(-2 - 3\,\mathrm{i}\,)}{13} = 1 - \mathrm{i};$$

thus $-2+3\,\mathrm{i}$ is a greatest common divisor of α and β.

(ii) By the computations above,

$$\begin{aligned}
\alpha &= \beta\cdot(-\,\mathrm{i}\,)+1+5\,\mathrm{i}\,,\\
1+5\,\mathrm{i}\, &= \alpha+\beta\cdot\,\mathrm{i}\,;\\
\beta &= (\alpha+\beta\cdot\,\mathrm{i}\,)(7+\,\mathrm{i}\,)-2+3\,\mathrm{i}\,,\\
-2+3\,\mathrm{i}\, &= \alpha\cdot(-7-\,\mathrm{i}\,)+\beta\cdot(2-7\,\mathrm{i}\,).
\end{aligned}$$

Remark. In (i), each step of the computation should lower the norm of the remainder. Indeed, $\mathrm{N}\,(39\,\mathrm{i}\,) > \mathrm{N}\,(1+5\,\mathrm{i}\,) > \mathrm{N}\,(-2+3\,\mathrm{i}\,)$. But the way to achieve this is not unique. For example, from the third line, the computation could have been

$$\begin{aligned}
\frac{39\,\mathrm{i}}{1+5\,\mathrm{i}} &= \frac{195+39\,\mathrm{i}}{26} = 8+\,\mathrm{i}\,+\frac{-1+\,\mathrm{i}}{2},\\
39\,\mathrm{i}\, &= (1+5\,\mathrm{i}\,)(8+\,\mathrm{i}\,)-3-2\,\mathrm{i}\,;\\
\frac{1+5\,\mathrm{i}}{-3-2\,\mathrm{i}} &= \frac{(1+5\,\mathrm{i}\,)(-3+2\,\mathrm{i}\,)}{13} = -1-\,\mathrm{i}\,.
\end{aligned}$$

So $-3-2\,\mathrm{i}$ could also be found as a greatest common divisor of α and β. (Also $2-3\,\mathrm{i}$ and $3+2\,\mathrm{i}$ are gcd's.)

In an alternative approach to (i), one might observe that

$$\begin{aligned}
\alpha &= 5\cdot(8+\,\mathrm{i}\,) = (2+\,\mathrm{i}\,)(2-\,\mathrm{i}\,)(8+\,\mathrm{i}\,),\\
\mathrm{N}\,(\alpha) &= 5^2\cdot 65 = 5^3\cdot 13;\\
\beta &= 3\cdot 13\,\mathrm{i}\,,\\
\mathrm{N}\,(\beta) &= 3^2\cdot 13^2.
\end{aligned}$$

The factors $2\pm\,\mathrm{i}$ of α are prime, and their norm is 5, and $5\nmid \mathrm{N}\,(\beta)$. Also, 3 is prime, and $3\nmid \mathrm{N}\,(\alpha)$. One can therefore take γ as a gcd of $8+\,\mathrm{i}$ and $13\,\mathrm{i}$. To find this, one could apply the Euclidean algorithm to the latter pair.

Instead of applying the Algorithm here, one may note that, since $\gcd(\mathrm{N}(\alpha), \mathrm{N}(\beta)) = 13$, we must have $\mathrm{N}(\gamma) \mid 13$. Since 13 has the prime factorization $(3 + 2\,\mathrm{i})(3 - 2\,\mathrm{i})$, each factor having norm 13, one could test whether one of these factors divides α and β: if one does, then it is γ; if neither does, then α and β are co-prime.

The alternative approaches are not much help in solving (ii). However, once one *does* have an answer to (ii), it is easy to check.

Problem 2. This problem involves the Diophantine equation

$$2x^2 - 3y^2 = 2. \tag{B.1}$$

(i) Express $\sqrt{3/2}$ as a continued fraction.

(ii) Find a positive solution to (B.1).

(iii) Find a solution (a, b) to (B.1) in which each of a and b has two digits (in the usual decimal notation).

(iv) Find a solution (a, b) to (B.1) in which each of a and b has three digits.

Solution. (i) Let $x = \sqrt{3/2} = \sqrt{6}/2$. Applying our algorithm to x, we have

$$\begin{aligned}
&& a_0 &= 1, & \xi_0 &= \frac{\sqrt{6}}{2} - 1 = \frac{\sqrt{6}-2}{2}; \\
\frac{2}{\sqrt{6}-2} &= \sqrt{6}+2, & a_1 &= 4, & \xi_2 &= \sqrt{6}-2; \\
\frac{1}{\sqrt{6}-2} &= \frac{\sqrt{6}+2}{2}, & a_2 &= 2, & \xi_2 &= \frac{\sqrt{6}-2}{2} = \xi_0;
\end{aligned}$$

therefore $\sqrt{3/2} = [1; \overline{4, 2}]$.

(ii) The equation (B.1) can be written as $x^2 - (3/2)y^2 = 1$. Assuming it is like a Pell equation, we expect solutions to $(*)$ to come from convergents of x. These are:

$$\frac{1}{1}, \quad \frac{5}{4}, \quad \frac{11}{9}, \quad \frac{49}{40}, \quad \frac{109}{89}, \quad \frac{485}{396}, \quad \dots$$

In particular, we expect the solutions to come from $[1;4]$, $[1;4,2,4]$, $[1;4,2,4,2]$, and so on. Indeed, $(5,4)$ is a solution.

(iii) Also $(49,40)$.

(iv) Also $(485,396)$.

Remark. Since we have not *yet* proved that our procedure for solving a Pell equation works in general, and since (B.1) is not literally a Pell equation anyway, one should check one's answers to (ii), (iii), and (iv) here.

Problem 3. In class we found the bijection

$$t \longmapsto \Big(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\Big)$$

between $\mathbb{Q}$ and the set of rational solutions (other than $(-1,0)$) to the equation

$$x^2 + y^2 = 1.$$

(i) Find all rational solutions to the equation

$$x^2 + 3y^2 = 1.$$

(ii) Find α in $\mathbb{Q}(\mathrm{i})$ such that $\mathrm{N}(\alpha) = 1$, but α is not a Gaussian integer.

(iii) Find β in $\mathbb{Q}(\sqrt{-3})$ such that $\mathrm{N}(\beta) = 1$, but β is not an integer (that is, not an Eisenstein integer).

Solution. (i) The solutions are $\left(\dfrac{1-3t^2}{1+3t^2}, \dfrac{2t}{1+3t^2}\right)$, where $t \in \mathbb{Q}$; and $(-1, 0)$.

(ii) Letting $t = 2$ in the given formula yields $(-3 + 4\,\mathrm{i}\,)/5$, not a Gaussian integer.

(iii) Letting $t = 2$ in (i) yields $(-11 + 4\,\mathrm{i}\,\sqrt{3})/13$, which is not in $\mathbb{Z}[(1 + \mathrm{i}\,\sqrt{3})/2]$.

Remark. One may solve (i) just by thinking about why the given point is on the circle. Alternatively, one may just use the same method for deriving it: find the other intersection, besides $(-1, 0)$ of the line $y = tx+t$ and the ellipse $x^2+3y^2 = 1$.

Problem 4. (i) Find all distinct solutions (from $\mathbb{Z}$) of the Diophantine equation

$$x^2 + y^2 = 221.$$

(ii) Find a factorization of $27-57\,\mathrm{i}$ as a product of Gaussian primes.

Solution. (i) $221 = 13{\cdot}17$. In the Gaussian integers, $\mathrm{N}\,(\xi) = 13$ is solved by $3\pm2\,\mathrm{i}$ and their associates; $\mathrm{N}\,(\eta) = 17$, by $4\pm\mathrm{i}$ and their associates. We have

$$(3 \pm 2\,\mathrm{i}\,)(4 \pm \mathrm{i}\,) = 10 \pm 11\,\mathrm{i}\,, \qquad (3 \pm 2\,\mathrm{i}\,)(4 \mp \mathrm{i}\,) = 14 \pm 5\,\mathrm{i}\,.$$

Hence the 16 desired solutions are

$$(10, \pm11), (-10, \mp11), (\mp11, 10), (\pm11, -10),$$
$$(14, \pm5), (-14, \mp5), (\mp5, 14), (\pm5, -14).$$

(ii) $27 - 57\,\mathrm{i} = 3 \cdot (9 - 19\,\mathrm{i}\,)$, where 3 is prime; and

$$\mathrm{N}\,(9 - 19\,\mathrm{i}\,) = 81 + 361 = 442 = 2 \cdot 221.$$

But 2 has associated prime factors $1 \pm \mathrm{i}$, and

$$\begin{aligned}\frac{9-19\,\mathrm{i}}{1+\mathrm{i}} = \frac{(9-19\,\mathrm{i})(1-\mathrm{i})}{2} &= -5-14\,\mathrm{i} \\ &= -\mathrm{i}\cdot(14-5\,\mathrm{i}) = -\mathrm{i}\cdot(3-2\,\mathrm{i})(4+\mathrm{i})\end{aligned}$$

by (i). Since $(1+\mathrm{i})\cdot(-\mathrm{i}) = 1-\mathrm{i}$, we conclude

$$27-57\,\mathrm{i} = 3\cdot(1-\mathrm{i})(3-2\,\mathrm{i})(4+\mathrm{i}).$$

B.2. May 26 (Monday)

Instructions. Solve four of these five problems in 90 minutes. *İyi çalışmalar.*

Problem 5. Assuming $a > 0$, prove

$$\sqrt{a^2+1} = [a;\overline{2a}].$$

Solution. By the algorithm for finding continued fractions, when $x = \sqrt{a^2+1}$, we have first $a_0 = a$, and then

$$\xi_0 = \sqrt{a^2+1} - a, \qquad \frac{1}{\xi_0} = \frac{\sqrt{a^2+1}+a}{a^2+1+a^2} = \sqrt{a^2+1}+a,$$

so $a_1 = 2a$ and $\xi_1 = \sqrt{a^2+1} - a = \xi_0$. Therefore $x = [a;\overline{2a}]$.

Remark. Alternatively, one may let

$$\begin{aligned}x = [a;\overline{2a}] = [a; a+a, \overline{2a}] = [a; a+[a,\overline{2a}]] \\ = [a; a+x] = a + \frac{1}{a+x} = \frac{a^2+ax+1}{a+x},\end{aligned}$$

so that $ax + x^2 = a^2 + ax + 1$ and therefore $x^2 = a^2+1$. Since $a > 0$, we have $[a;\overline{2a}] > 0$ and therefore $[a;\overline{2a}] = x = \sqrt{a^2+1}$.

Problem 6. Let $K = \mathbb{Q}(\sqrt{5})$ and $\Lambda = \langle 1, \sqrt{5} \rangle$.

(i) Find the order $\mathfrak{O}_\Lambda$ (that is, $\{\xi \in K : \xi\Lambda \subseteq \Lambda\}$).

(ii) Find the elements of $\mathfrak{O}_\Lambda$ having norm 1.

Solution. (i) Since $\sqrt{5}$ is a root of $x^2 - 5$, whose leading coefficient is 1, we can conclude $\mathfrak{O}_\Lambda = \langle 1, \sqrt{5} \rangle = \Lambda$.

(ii) We know that the units of $\mathfrak{O}_K$ (when $K = \mathbb{Q}(\sqrt{5})$) are $\pm\phi^n$. Of these, those that are greater than 1 form the list

$$\phi, 1 + \phi, 1 + 2\phi, 2 + 3\phi, 3 + 5\phi, 5 + 8\phi, \ldots$$

(and in general $\phi^n = \mathrm{F}_{n-1} + \mathrm{F}_n\phi$). But since $2\phi = 1 + \sqrt{5}$, we have $\mathfrak{O}_\Lambda = \langle 1, 2\phi \rangle$; also, $\mathrm{N}(\phi) = -1$. The first power of ϕ greater than 1 that belongs to $\mathfrak{O}_\Lambda$ and has norm 1 is therefore ϕ^6. Hence the elements of $\mathfrak{O}_\Lambda$ of norm 1 are $\pm\phi^{6n}$, where $n \in \mathbb{Z}$.

Problem 7. Solve in $\mathbb{Z}$:

$$x^2 + 2xy + 4y^2 = 19.$$

Solution. We want to solve

$$19 = x^2 + 2xy + 4y^2 = (x + y)^2 + 3y^2.$$

Hence $y^2 \leqslant 19/3 < 9$, so $|y| < 3$. When $y = \pm 2$, the equation becomes $(x \pm 2)^2 = 7$, which has no solution. When $y = \pm 1$, we get $(x \pm 1)^2 = 16$, so $(x \pm 1) \in \{4, -4\}$. When $y = 0$, there is no solution. So the solutions of the original equation are $(3, 1)$, $(-5, 1)$, $(5, -1)$, $(-3, -1)$.

Remark. Solving an equation means not only finding solutions, but showing that there are no other solutions. This is done here by noting that there are only 5 possibilities for y. Alternatively, one may rewrite the equation as

$$19 = (x + y + y\sqrt{-3})(x + y - y\sqrt{-3}) = \mathrm{N}\,(x + 2\omega y)\,,$$

where we work in $\mathbb{Q}(\sqrt{-3})$. Since (x, y) is a solution if and only if $(|x|, |y|)$ is a solution, we can obtain all solutions from Figure B.1.

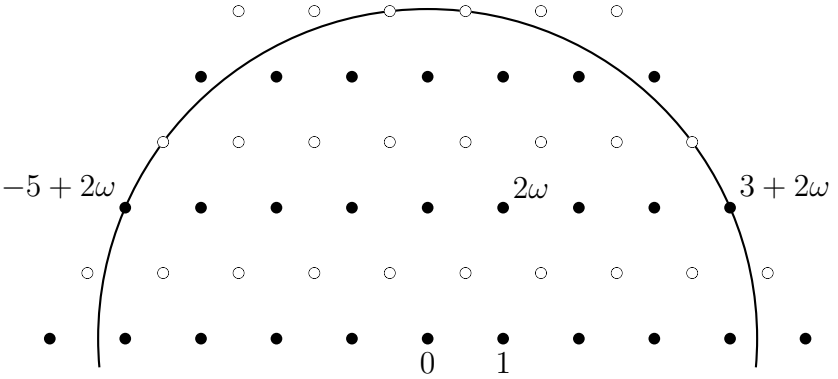

Figure B.1.: Solutions of $\mathrm{N}\,(\xi) = 19$ from $\langle 1, 2\omega\rangle$ in $\mathbb{Q}(\sqrt{-3})$

Problem 8. (i) Prove that, for each n in $\mathbb{Z}$, there are a_n and b_n in $\mathbb{Z}$ such that

$$a_n + b_n\sqrt{21} = 2\Big(\frac{5 + \sqrt{21}}{2}\Big)^n.$$

(ii) Find a quadratic form $f(x, y)$ and a rational integer m such that each $(\pm a_n, \pm b_n)$ is a solution of

$$f(x, y) = m. \tag{B.2}$$

(iii) Prove that each solution of (B.2) is $(\pm a_n, \pm b_n)$ for some n.

Solution. (i) In $\mathbb{Q}(\sqrt{21})$, we have $(5+\sqrt{21})/2 = 2+\omega$, and $\mathrm{N}\big((5+\sqrt{21})/2\big) = 1$. Hence $(5+\sqrt{21})/2$ is a unit of $\mathfrak{O}_K$, so its powers are also units of $\mathfrak{O}_K$. Let $\alpha \in \mathfrak{O}_K$. Since

$$\mathfrak{O}_K = \langle 1, \omega \rangle = \Big\langle 1, \frac{1+\sqrt{21}}{2} \Big\rangle,$$

we have $2\alpha \in \langle 2, 1+\sqrt{21} \rangle \subseteq \langle 1, \sqrt{21} \rangle$. This proves

$$a_n + b_n\sqrt{21} = 2\Big(\frac{5+\sqrt{21}}{2}\Big)^n \in \langle 1, \sqrt{21} \rangle,$$

so $a_n, b_n \in \mathbb{Z}$.

(ii) Since $\mathrm{N}\big(a_n + b_n\sqrt{21}\big) = 4$, the pairs $(\pm a_n, \pm b_n)$ are solutions of $x^2 - 21y^2 = 4$.

(iii) Suppose (a, b) is an arbitrary solution of $x^2 - 21y^2 = 4$. Then $a \equiv b \pmod 2$, so $2 \mid a-b$. Hence

$$\begin{aligned} \frac{a+b\sqrt{21}}{2} &= \frac{a-b+b+b\sqrt{21}}{2} \\ &= \frac{a-b}{2} + b\frac{1+\sqrt{21}}{2} = \frac{a-b}{2} + b\omega \in \langle 1, \omega \rangle, \end{aligned}$$

so $(a+b\sqrt{21})/2$ is an element of $\mathfrak{O}_K$ of norm 1. But there is ε or $r+s\omega$ in $\mathfrak{O}_K$ of norm 1 such that $r, s > 0$ and every element of $\mathfrak{O}_K$ of norm 1 is $\pm\varepsilon^n$ for some n. But $(5+\sqrt{21})/2 = 2+\omega$ and has norm 1, so it must be ε. Hence $(a, b) = (\pm a_n, \pm b_n)$ for some n.

Remark. The pair $(a_n/2, b_n/2)$ solves the Pell equation $x^2 - 21y^2 = 1$, but its entries need not belong to $\mathbb{Z}$. For example, $(a_1/2, b_1/2) = (5/2, 1/2)$.

Problem 9. (i) Find a quadratic field K, a lattice $\langle \alpha, \beta \rangle$ or Λ of K, and m in $\mathbb{Z}$ for which the function

$$(x, y) \mapsto x\alpha + y\beta$$

is a bijection between the solution-set (in $\mathbb{Z} \times \mathbb{Z}$) of

$$2x^2 - 3y^2 = 2 \tag{B.3}$$

and the solution-set in Λ of $\mathrm{N}(\xi) = m$.

(ii) Describe a parallelogram Π in the plane $\mathbb{R}^2$ such that, for every solution (a, b) of (B.3), there is a solution (c, d) in Π such that

$$\frac{a\alpha + b\beta}{c\alpha + d\beta} \in \mathfrak{O}_\Lambda. \tag{B.4}$$

(iii) Find Π as in (ii) with the additional condition that, if (a, b) and (c, d) are distinct solutions to (B.3) in Π, then (B.4) fails.

Solution. (i) We have $2 = 2x^2 - 3y^2 \iff 4 = 4x^2 - 6y^2 = \mathrm{N}\left(2x + y\sqrt{6}\right)$ in $\mathbb{Q}(\sqrt{6})$. So let

$$K = \mathbb{Q}(\sqrt{6}), \quad \alpha = 2, \quad \beta = \sqrt{6}, \quad m = 4.$$

(ii) We want the elements of $\mathfrak{O}_\Lambda$ of norm 1. But $(1/2)\Lambda = \langle 1, \sqrt{6}/2 \rangle$, and $\sqrt{6}/2$ is a root of $2x^2 - 3$. Hence

$$\mathfrak{O}_\Lambda = \langle 1, 2\sqrt{6}/2 \rangle = \langle 1, \sqrt{6} \rangle = \langle 1, \omega \rangle = \mathfrak{O}_K.$$

We obtain the units of $\mathfrak{O}_K$ from the continued-fraction expansion of $\sqrt{6}$:

$$\begin{aligned}
x &= \sqrt{6}, & a_0 &= 2, & \xi_0 &= \sqrt{6} - 2; \\
\frac{1}{\xi_0} &= \frac{\sqrt{6} + 2}{2}, & a_1 &= 2, & \xi_1 &= \frac{\sqrt{6} - 2}{2}; \\
\frac{1}{\xi_1} &= \sqrt{6} + 2, & a_2 &= 4, & \xi_2 &= \sqrt{6} - 2 = \xi_0;
\end{aligned}$$

so $\sqrt{6} = [2; \overline{2, 4}]$. Since $[2; 2] = 5/2$, and $\mathrm{N}\,(5 + 2\omega) = 1$, we can conclude that the elements of $\mathfrak{O}_K$ of norm 1 are $\pm(5+2\omega)^n$. Therefore the desired parallelogram $\mathit{\Pi}$ can be bounded by the straight lines given by

$$2x + y\sqrt{6} = 1; \qquad 2x + y\sqrt{6} = 5 + 2\sqrt{6}.$$

Also, we are looking for points on the hyperbola

$$4 = 4x^2 - 6y^2 = (2x + y\sqrt{6})(2x - y\sqrt{6}),$$

one of whose asymptotes, given by

$$2x - y\sqrt{6} = 0,$$

forms a third side of $\mathit{\Pi}$; the fourth side is given by

$$2x - y\sqrt{6} = 4,$$

since this line meets the hyperbola where $2x + y\sqrt{6} = 1$ does.

(iii) Same as (ii).

Remark. The point in (ii) is that, if γ is from $\mathit{\Lambda}$ and solves $\mathrm{N}\,(\xi) = 4$, then the same is true of δ or $2a + b\omega$, where $\delta = \pm(5 + 2\omega)^n\gamma$; and we should be able to pick the sign and n so that $(a, b) \in \mathit{\Pi}$. But we can pick n so that

$$1 \leqslant |\delta| < |5 + 2\omega| < 10.$$

We also have $4 = \delta\delta'$, so

$$|\delta'| = \frac{4}{\delta} \leqslant 4.$$

Since

$$\delta = \frac{\delta + \delta'}{2} + \frac{\delta - \delta'}{2\omega}\omega.$$

we conclude

$$|a| = \left|\frac{\delta + \delta'}{4}\right| < 4, \quad |b| = \left|\frac{\delta - \delta'}{2\omega}\right| < 4.$$

Thus, in (ii), Π can be the square with vertices $(\pm 4, 4)$ and $(\pm 4, -4)$. But this isn't good enough for (iii).

B.3. June 2, 2008 (Monday)

Problem 10. Suppose $\sqrt{2} = [a_0; a_1, a_2, \dots]$, and as usual let $p_n/q_n = [a_0; a_1, \dots, a_n]$. Find rational integers a, b, k, and ℓ such that

$$p_n + q_n\sqrt{2} = (a + b\sqrt{2})(k + \ell\sqrt{2})^n$$

for all positive rational integers n.

Solution. First compute the expansion of $\sqrt{2}$:

$$\begin{aligned} & & a_0 &= 1, & \xi_0 &= \sqrt{2} - 1; \\ \frac{1}{\sqrt{2}-1} &= \sqrt{2} + 1, & a_1 &= 2, & \xi_1 &= \sqrt{2} - 1 = \xi_0. \end{aligned}$$

So $\sqrt{2} = [1, \overline{2}]$. In particular, the period has length 1, so

$$p_{n+1} + q_{n+1}\sqrt{2} = (p_n + q_n\sqrt{2})(p_0 + q_0\sqrt{2}).$$

Since $p_0/q_0 = 1/1$, we conclude

$$p_n + q_n\sqrt{2} = (1 + \sqrt{2})(1 + \sqrt{2})^n.$$

(This is justified by Theorem 20 of the notes. Alternatively, one may note that

$$\frac{p_{n+1}}{q_{n+1}} = \left[1, 1 + \frac{p_n}{q_n}\right] = 1 + \frac{q_n}{p_n + q_n} = \frac{p_n + 2q_n}{p_n + q_n},$$

and both fractions are irreducible, so $(p_n + q_n\sqrt{2})(1+\sqrt{2}) = p_n + 2q_n + (p_n+q_n)\sqrt{2} = p_{n+1} + q_{n+1}\sqrt{2}$.)

Problem 11. Here Λ and M are lattices in some quadratic field.

(i) Find $|\Lambda/M|$, that is, $(\Lambda : M)$, when

a) $\Lambda = \langle \alpha, \beta \rangle$, $M = \langle 2\alpha, 3\beta \rangle$;

b) $\Lambda = \langle \alpha, \beta \rangle$, $M = \langle 2\alpha, \alpha + 3\beta \rangle$.

(ii) Assuming $M \subseteq \Lambda$, find a number n such that $n\Lambda \subseteq M$.

Solution. (i) a) 6. b) 6.

(ii) Let $n = (\Lambda : M)$. Indeed, we can write Λ as $\langle \alpha, \beta \rangle$, and then $M = \langle c\alpha, f\alpha + e\beta \rangle$ for some positive rational integers c, e, and f. Then $(\Lambda : M) = ce$, and $ce\Lambda = \langle ce\alpha, ce\beta \rangle \subseteq M$ since $ce\beta = c(f\alpha + e\beta) - f(c\alpha)$.

Problem 12. In some quadratic field, find a lattice Λ such that $\mathrm{N}(\Lambda) = 1$, but $\Lambda \neq \mathfrak{O}_\Lambda$.

Solution. One strategy is to find a lattice $\langle \alpha, \beta \rangle$ whose norm is k^2 for some k; then Λ can be $\langle \alpha/k, \beta/k \rangle$. Assuming the quadratic field K is $\mathbb{Q}(\sqrt{d})$, where $d \equiv 2$ or $3 \pmod 4$, we can try letting $\langle \alpha, \beta \rangle = \langle k^2, \ell + \sqrt{d} \rangle$, where ℓ will be chosen so that the order is $\langle 1, \sqrt{d} \rangle$, that is, $\mathfrak{O}_K$. To compute this order, we have

$$\begin{aligned} x = \frac{\ell + \sqrt{d}}{k^2} &\implies k^2 x - \ell = \sqrt{d} \\ &\implies k^4 x^2 - 2k^2 \ell x + \ell^2 - d = 0 \\ &\implies k^2 x^2 - 2\ell x + \frac{\ell^2 - d}{k^2} = 0. \end{aligned}$$

It is enough now if $\gcd(k, 2\ell) = 1$, while $k^2 \mid \ell^2 - d$. We can achieve this by letting $k = 3$, $\ell = 5$, and $d = -2$. So

$$\Lambda = \left\langle 3, \frac{5 + \sqrt{-2}}{3} \right\rangle$$

is one possibility.

Problem 13. Letting $K = \mathbb{Q}(\sqrt{5})$ and $\mathfrak{O} = \mathfrak{O}_K$, for each p in $\{2, 3, 5, 7, 11\}$, find the prime factorization of $p\mathfrak{O}$ in $\mathfrak{O}$.

Solution. In the notation of our last theorem, $\Delta = d = 5$. Then 5 ramifies in $\mathfrak{O}$, and

$$5\mathfrak{O} = \left\langle 5, \frac{5 + \sqrt{5}}{2} \right\rangle^2.$$

Now we check solubility of $5 \equiv x^2 \pmod{4p}$ for the remaining p. There is no solution when $p \in \{2, 3, 7\}$. Indeed, when $p = 2$, just check the possibilities: $(\pm 1)^2 \equiv 1$; $(\pm 2)^2 \equiv 4$; $(\pm 3)^2 \equiv 1$; $4^2 \equiv 0$. In the other cases, we can show $5 \equiv x^2 \pmod{p}$ is insoluble by Legendre symbols and quadratic reciprocity: $(5/3) = (2/3) = -1$; $(5/7) = (7/5) = (2/5) = -1$. So 2, 3, and 7 are inert in $\mathfrak{O}$.

Finally, $(5/11) = (11/5) = (1/5) = 1$, and indeed $5 \equiv 7^2 \pmod{44}$. Then

$$11\mathfrak{O} = \left\langle 11, \frac{7 + \sqrt{5}}{2} \right\rangle \left\langle 11, \frac{7 - \sqrt{5}}{2} \right\rangle.$$

Bibliography

[1] William W. Adams and Larry Joel Goldstein. *Introduction to number theory*. Prentice-Hall, Englewood Cliffs, N.J., 1976.

[2] Apollonius of Perga. *Apollonii Pergaei Qvae Graece Exstant Cvm Commentariis Antiqvis*, volume I. Teubner, 1974. Edited with Latin interpretation by I. L. Heiberg. First published 1891.

[3] Apollonius of Perga. *Conics. Books I–III*. Green Lion Press, Santa Fe, NM, revised edition, 1998. Translated and with a note and an appendix by R. Catesby Taliaferro, with a preface by Dana Densmore and William H. Donahue, an introduction by Harvey Flaumenhaft, and diagrams by Donahue, edited by Densmore.

[4] David M. Burton. *Elementary Number Theory*. McGraw-Hill, Boston, sixth edition, 2007.

[5] Graham Everest and Thomas Ward. *An introduction to number theory*, volume 232 of *Graduate Texts in Mathematics*. Springer-Verlag London, London, 2005.

[6] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Clarendon Press, Oxford, fifth edition, 1979. First edition 1938. Reprinted 1990.

[7] D. Hilbert and S. Cohn-Vossen. *Geometry and the imagination*. Chelsea Publishing, New York, 1952. Translated by P. Neményi.

[8] Edmund Landau. *Elementary Number Theory*. Chelsea Publishing, New York, 1958. Originally part of *Vorlesungen über Zahlentheorie* (Leipzig, 1927). Translated by J. E. Goodman.

[9] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[10] James E. Shockley. *Introduction to number theory*. Holt Rinehart and Winston, New York, 1967.

Index

K (a quadratic field, usually $\mathbb{Q}(\sqrt{d})$), 33
$\mathbb{C}$ (the field of complex numbers), 33
$\mathrm{End}(\Lambda)$, 51
F_n, 83
$\mathbb{Q}$ (the field of rational numbers), 20
$\mathbb{Q}(\sqrt{d})$, 34
$\mathbb{R}$ (the field of real numbers), 54
$\mathbb{Z}$ (the ring of rational integers), 35
$\Delta(\Lambda)$, $\Delta(\alpha, \beta)$, 64
$\mathrm{d}(x)$, 37
ε_Λ, 81
$\mathbb{Z}[\mathrm{i}]$ (the ring of Gaussian integers), 35
ϕ (the Golden Ratio), 83
$\langle \alpha, \beta \rangle$, 51
Δ, 127
i (not the variable i, but $\sqrt{-1}$), 15
π (the circumference of the unit circle), 44
$\mathrm{N}(x)$, 36, 45
ω (generator of $\mathfrak{O}_K$ over $\mathbb{Z}$), 48
$\mathfrak{O}_\Lambda$, 68
π (an arbitrary prime of $\mathbb{Z}[\mathrm{i}]$), 41
$\mathfrak{O}_K$, 46
$\mathrm{Tr}(x)$, 45
ω, 24
ω (the set $\{x \in \mathbb{Z} \colon x \geqslant 0\}$), 37
d (a square-free element of $\mathbb{Z}$, not 1), 45

algebraic integer, 35
associate, 39

belong, 113
binary quadratic form, 49

conductor, 69
conjugate, 75
continued fraction, 20, 21, 25
convergent, 25

degree, 37

diameter, 75
Diophantine equation, 11
discriminant, 50, 64
divisibility, 121
domain, 37
doubly periodic, 54

Eisenstein integer, 132
elliptic curve, 55
endomorphism, 51
Euclidean algorithm, 24
Euclidean domain, 37

Fibonacci number, 83
free abelian subgroup, 51
fundamental unit, 81

Gaussian integer, 35
Golden Ratio, 83
greatest common divisor, 39, 122

ideal, 112, 113
inert, 126
infinite descent, 14
integer, 35
integral, 114
integral domain, 37
irreducible, 40, 121

lattice, 38, 51
limit, 22

minimal polynomial, 46

norm, 36, 45, 113

order, 68, 113

Pell equation, 29
positive, 31
prime, 41, 121, 122
primitive solution, 12
principal-ideal domain, 40
Pythagorean triple, 13

quadratic extension, 11
quadratic field, 33

ramify, 126
rational integer, 35
rational point, 19

simple, 25
split, 126
square-free, 33

torus, 54
trace, 45
transverse, 85

unique-factorization domain, 40
upright, 85

Weierstraß function, 54