

# **Number Theory 2**

Paul Yiu

Department of Mathematics  
Florida Atlantic University

Spring 2007



# Contents

<b>1 Preliminaries</b>	<b>101</b>
1.1 Infinitude of prime numbers . . . . .	101
1.2 Euclidean algorithm and linear Diophantine equations .	101
1.2.1 Euclidean Algorithm . . . . .	101
1.3 The greatest common divisor . . . . .	102
1.3.1 $\gcd(a, b)$ as an integer combination of $a$ and $b$ . .	103
1.3.2 Linear Diophantine equations . . . . .	103
1.4 Chinese remainder theorem . . . . .	104
1.5 Fermat's little theorem and the Euler $\varphi$ -function . . . .	104
1.6 Some number theoretic functions . . . . .	105
<b>2 Pythagorean triangles</b>	<b>201</b>
2.1 Construction of Pythagorean triangles . . . . .	201
2.2 Primitive Pythagorean triangles with consecutive legs .	202
2.3 Fermat Last Theorem for $n = 4$ . . . . .	204
2.4 Nonexistence of a pair of Pythagorean triangles with legs $a, b$ , and $a, 2b$ . . . . .	206
2.5 Impossibility of 4 squares in arithmetic progression . .	207
<b>3 Homogeneous quadratic equations in 3 variables</b>	<b>213</b>
3.1 Pythagorean triangles revisited . . . . .	213
3.2 Rational points on a conic . . . . .	214
<b>4 Integer triangles with a <math>60^\circ</math> or <math>120^\circ</math> angle</b>	<b>215</b>
4.1 Integer triangles with a $60^\circ$ angle . . . . .	215
4.2 Integer triangles with a $120^\circ$ angle . . . . .	217
4.3 A pair of discordant forms: $x^2 \pm xy + y^2$ . . . . .	219

<b>5</b>	<b>Heron triangles</b>	<b>221</b>
5.1	The Heron formula . . . . .	221
5.2	Heron triangles . . . . .	222
5.3	Construction of Heron triangles . . . . .	223
5.4	Heron triangles with sides in arithmetic progression . . . . .	224
5.5	Heron triangles with integer inradii . . . . .	225
5.6	Impossibility of a Heron triangle with one side twice another . . . . .	226
<b>6</b>	<b>Sums of two and four squares</b>	<b>301</b>
6.1	Euler's proof of Fermat's two-square theorem . . . . .	301
6.2	Representation of integers as sums of two squares . . . . .	302
6.3	Lagrange's proof of the four-square theorem . . . . .	303
6.3.1	Descent . . . . .	303
<b>7</b>	<b>Finite continued fractions</b>	<b>305</b>
7.1	Euler's function for the convergents of a continued fraction . . . . .	305
7.2	Cornacchia' algorithm for a prime as a sum of two squares	307
<b>8</b>	<b>Quadratic Residues</b>	<b>401</b>
8.1	The Legendre symbol . . . . .	403
8.2	The law of quadratic reciprocity . . . . .	406
8.3	Calculation of square roots modulo $p$ . . . . .	409
8.4	Square roots modulo an odd prime power . . . . .	411
8.5	Square modulo $2^k$ . . . . .	412
<b>9</b>	<b>The ring of Gaussian integers</b>	<b>501</b>
9.1	The ring $\mathbb{Z}[i]$ . . . . .	501
9.1.1	Norm and units . . . . .	501
9.1.2	Gaussian primes . . . . .	501
9.2	An alternative proof of Fermat's two-square theorem . . . . .	503
<b>10</b>	<b>Construction of indecomposable Heron triangles</b>	<b>505</b>
10.1	Primitive Heron triangles . . . . .	505
10.1.1	Rational triangles . . . . .	505
10.1.2	Triple of simplifying factors . . . . .	506
10.1.3	Decomposition of Heron triangles . . . . .	507
10.2	Gaussian integers . . . . .	508
10.2.1	Heron triangles and Gaussian integers . . . . .	509

10.3	Orthocentric Quadrangles . . . . .	511
10.4	Indecomposable primitive Heron triangles . . . . .	512
10.4.1	Construction of Heron triangles with given simplifying factors . . . . .	513
<b>11</b>	<b>Infinite continued fractions</b>	<b>601</b>
11.1	Lagrange's Theorem . . . . .	604
11.1.1	Purely periodic continued fractions. . . . .	604
11.1.2	Eventually periodic continued fractions . . . . .	604
11.1.3	Reduced quadratic irrationalities . . . . .	605
11.1.4	Proof of Lagrange's theorem . . . . .	606
<b>12</b>	<b>The Pell Equation</b>	<b>609</b>
12.1	The equation $x^2 - dy^2 = 1$ . . . . .	609
12.1.1	. . . . .	611
12.2	The equation $x^2 - dy^2 = -1$ . . . . .	612
12.3	The equation $x^2 - dy^2 = c$ . . . . .	612
12.4	Applications . . . . .	614
<b>13</b>	<b>Elliptic Curves</b>	<b>701</b>
13.1	Group law on $y^2 = x^3 + ax^2 + bx + c$ . . . . .	701
13.2	The discriminant . . . . .	702
<b>14</b>	<b>Heron triangles and Elliptic Curves</b>	<b>705</b>
14.1	The elliptic curve $y^2 = (x - k)^2 - 4kx^3$ . . . . .	705
14.1.1	Proof of Theorem 14.1 . . . . .	708
14.1.2	Theorem 11.4 . . . . .	904



# Chapter 1

## Preliminaries

### 1.1 Infinitude of prime numbers

You certainly know that there are infinitely many primes. You should know how to explain this; I mean Euclid's beautiful proof. There are indeed many other proofs. Here is one which appeared most recently ([16]).

Let  $n$  be an arbitrary positive integer  $> 1$ . Since  $n$  and  $n + 1$  are consecutive integers, they are relatively prime. Hence, the number  $N_2 := n(n + 1)$  must have two different prime divisors. Similarly, since  $N_2$  and  $N_2 + 1$  are consecutive, and therefore relatively prime, the number  $N_3 := N_2(N_2 + 1)$  must have at least three distinct prime divisors. If we continue by setting

$$N_{k+1} = N_k(N_k + 1), \quad N_1 = n,$$

then by induction,  $N_k$  has at least  $k$  distinct prime divisors. It follows that the number of primes exceeds any finite integer.

### 1.2 Euclidean algorithm and linear Diophantine equations

#### 1.2.1 Euclidean Algorithm

The euclidean algorithm affirms that in every division of integers, there is a unique quotient and a unique remainder, under the stipulation that the remainder must be smaller than the divisor.

**Theorem 1.1.** *Given integers  $a$  and  $b \neq 0$ , there are unique integers  $q$  and  $r$  satisfying*

$$a = bq + r, \quad 0 \leq r < |b|. \quad (1.1)$$

If  $r = 0$ , we say that  $a$  is divisible by  $b$ , or simply that  $b$  divides  $a$ , and write  $b|a$ .

### 1.3 The greatest common divisor

Suppose  $a = bq + c$  for integers  $a, b, c$ , and  $q$ . It is easy to see that every common divisor of  $a$  and  $b$  is a common divisor of  $b$  and  $c$ , and *conversely*. We define the *greatest common divisor* of two positive integers  $a$  and  $b$  to be the greatest element of the (nonempty) set of common divisors of  $a$  and  $b$ , denoted by  $\gcd(a, b)$ . Clearly, if  $b|a$ , then  $\gcd(a, b) = b$ . In general, from (1.1), we have  $\gcd(a, b) = \gcd(b, r)$ . These observations lead to a straightforward calculation of the gcd of two numbers. To be systematic, we write  $a = r_{-1}$  and  $b = r_0$  (assumed positive).

$$\begin{aligned} r_{-1} &= r_0 q_0 + r_1, & 0 \leq r_1 < r_0, \\ r_0 &= r_1 q_1 + r_2, & 0 \leq r_2 < r_1, \\ r_1 &= r_2 q_2 + r_3, & 0 \leq r_3 < r_2, \\ r_2 &= r_3 q_3 + r_4, & 0 \leq r_4 < r_3, \\ & \vdots \end{aligned}$$

This division process eventually terminates since the remainders get smaller and smaller

$$r_{-1} > r_0 > r_1 > r_2 > \cdots$$

and yet remain nonnegative. In other words, some  $r_n$  divides the preceding  $r_{n-1}$  (and leaves a remainder  $r_{n+1} = 0$ ).

$$\begin{aligned} & \vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n. \end{aligned}$$

From these,

$$r_n = \gcd(r_{n-1}, r_n) = \gcd(r_{n-2}, r_{n-1}) = \cdots = \gcd(r_{-1}, r_0) = \gcd(a, b).$$

**1.3.1 gcd( $a, b$ ) as an integer combination of  $a$  and  $b$ .**

The above calculation of  $\text{gcd}(a, b)$  can be retraced to give  $\text{gcd}(a, b)$  as an integer combination of  $a$  and  $b$ . We augment the table of calculations with two extra rows of integers  $x_k$  and  $y_k$  obtained from  $q_{k-1}$  in the same way as  $r_k$ , beginning with  $(x_{-1}, x_0) = (1, 0)$  and  $(y_{-1}, y_0) = (0, 1)$ :

$$\begin{aligned} x_k &= x_{k-2} - q_{k-1}x_{k-1}, & x_{-1} &= 1, & x_0 &= 0; \\ y_k &= y_{k-2} - q_{k-1}y_{k-1}, & y_{-1} &= 0, & y_0 &= 1. \end{aligned}$$

The calculation of  $\text{gcd}(a, b)$ , and its expression in terms of  $a$  and  $b$ , can be efficiently performed by completing the following table.

$k$	-1	0	1	2	...	$n-1$	$n$
$r_k$	$a$	$b$	$r_1 = a - bq_0$	$r_2 = b - r_1q_1$	...	$r_{n-1}$	$r_n = \text{gcd}$
$q_k$	*	*	$q_0$	$q_1$	...	$q_{n-1}$	$q_n$ exactly divides
$x_k$	1	0					
$y_k$	0	1					

In each of these steps,  $r_k = ax_k + by_k$ . In particular,

$$\text{gcd}(a, b) = r_n = ax_n + by_n.$$

It can be proved that  $|x_n| < b$  and  $|y_n| < a$ .

**1.3.2 Linear Diophantine equations**

**Theorem 1.2.** *Let  $a, b, c$  be integers,  $a$  and  $b$  nonzero. Consider the linear Diophantine equation*

$$ax + by = c. \tag{1.2}$$

1. *The equation (1.2) is solvable in integers if and only if  $d := \text{gcd}(a, b)$  divides  $c$ .*
2. *If  $(x, y) = (x_0, y_0)$  is a particular solution of (1.2), then every integer solution is of the form*

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t,$$

where  $t$  is an integer.

3. *For  $c = \text{gcd}(a, b)$ , a particular solution  $(x, y) = (x_0, y_0)$  of (1.2) can be found such that  $|x_0| < |b|$  and  $|y_0| < |a|$ .*

## 1.4 Chinese remainder theorem

You should know the Chinese remainder theorem as an explicit method of calculation.

**Theorem 1.3 (Chinese remainder theorem).** *If  $m_1, m_2, \dots, m_k$  are pairwise relatively prime integers, then the simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

*has a unique solution  $x \pmod{m}$ , where  $m = m_1 m_2 \cdots m_k$ .*

This solution  $x$  is found by solving  $k$  similar but simpler problems, each time replacing  $a_1, \dots, a_k$  by one 1 and all others 0. For  $j = 1, 2, \dots, k$ , find a number  $b_j$  satisfying

$$b_j \equiv \begin{cases} 1 & \pmod{m_i}, \quad i = j, \\ 0 & \pmod{m_i}, \quad i \neq j. \end{cases}$$

Such a number must be a multiple of  $m_1 \cdots \widehat{m_j} \cdots m_k$ . With such numbers  $b_1, \dots, b_k$ , the solution to the system of simultaneous congruences above is then given by

$$x \equiv a_1 b_1 + a_2 b_2 + \cdots + a_k b_k \pmod{m}.$$

## 1.5 Fermat's little theorem and the Euler $\varphi$ -function

**Theorem 1.4 (Fermat's little theorem).** *If  $p$  is a prime number and  $p \nmid a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .*

There is a very important generalization involving the Euler  $\varphi$ -function

$$\varphi(n) := |\{k \in \mathbb{Z} : 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\}|.$$

**Theorem 1.5.** If  $\gcd(a, n) = 1$ , then  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

*Proof.* Let  $m = \varphi(n)$  and

$$a_1, a_2, \dots, a_m$$

be the  $m$  integers in the range  $[1, n]$  relatively prime to  $n$ . If  $\gcd(a, n) = 1$ , then

$$a \cdot a_1, a \cdot a_2, \dots, a \cdot a_m$$

represent exactly the same  $m$  congruence classes mod  $n$ . Therefore,

$$a^m \prod_{i=1}^k a_i = \prod_{i=1}^k (a \cdot a_i) \equiv \prod_{i=1}^k a_i \pmod{n}.$$

Cancelling the common invertible congruence class  $\prod_{i=1}^k a_i$ , we have  $a^m \equiv 1 \pmod{n}$ .  $\square$

## 1.6 Some number theoretic functions

**Theorem 1.6 (Unique factorization).** Every positive integer  $> 1$  is uniquely the product of distinct prime powers:

$$n = \prod_{i=1}^k p_i^{a_i}.$$

Here are three important number theoretic functions.

1. The number of divisors function:  $d(n) := |\{d \in \mathbb{N} : d|n\}|$ .
2. The sum of divisors function:  $\sigma(n) := \sum_{d|n} d$ .
3. Euler  $\varphi$ -function:  $\varphi(n) := |\{k \in \mathbb{Z} : 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\}|$ .

Each of these functions is multiplicative, *i.e.*,  $f(mn) = f(m)f(n)$  if  $\gcd(m, n) = 1$ . They are therefore determined by their values at the prime powers.

1.  $d(p^a) = 1 + a$ ;
2.  $\sigma(p^a) = 1 + p + \dots + p^a = \frac{p^{a+1}-1}{p-1}$ ;
3.  $\varphi(p^a) = p^a - p^{a-1} = p^a \left(1 - \frac{1}{p}\right)$ .

### Appendix: Perfect numbers

A perfect number is an integer equal to the sum of all of its divisors, including 1 but excluding the number itself. Euclid had given the following rule of construction of *even* perfect numbers. If  $M_k := 1 + 2 + \cdots + 2^{k-1} = 2^k - 1$  is a prime number,<sup>1</sup> then the number  $N_k := 2^{k-1}M_k$  is perfect. Now, in terms of the function  $\sigma$ , an integer  $n$  is perfect if  $\sigma(n) = 2n$ . Here is an easy proof of Euclid's construction:

$$\begin{aligned}\sigma(N_k) &= \sigma(2^{k-1}M_k) = \sigma(2^{k-1})\sigma(M_k) = (2^k - 1)(1 + M_k) \\ &= M_k \cdot 2^k = 2 \cdot 2^{k-1}M_k = 2N_k.\end{aligned}$$

Therefore,  $N_k$  is an even perfect number perfect.

Euler has subsequently shown that every even perfect number must be for this form.<sup>2</sup>

Let  $N$  be an *even* perfect number, factored into the form  $N = 2^{k-1} \cdot m$ , where  $k - 1 \geq 1$  and  $m$  is odd. Thus,

$$2N = \sigma(N) = \sigma(2^{k-1} \cdot m) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m).$$

It follows that

$$\sigma(m) = \frac{2N}{2^k - 1} = \frac{2^k}{2^k - 1} \cdot m = m + \frac{m}{2^k - 1}.$$

Note that the number  $\frac{m}{2^k - 1}$ , being the difference  $\sigma(m) - m$ , is an integer. As such, it is a divisor of  $m$ . This expression shows that  $m$  has **exactly** two divisors. From this we conclude that  $\frac{m}{2^k - 1} = 1$  and  $m = 2^k - 1$  is a prime. This means that every even perfect number must be of the form  $2^{k-1}(2^k - 1)$  in which the factor  $2^k - 1$  is a prime. This was exactly what Euclid gave.

---

<sup>1</sup>The number  $M_k = 2^k - 1$  is usually known as the  $k$ -th Mersenne number. There are only 44 known Mersenne primes. The latest and greatest record is  $M_{32582657}$  which has 9808358 digits. It is also the greatest known prime.

<sup>2</sup>It is not known if an odd perfect number exists.

## Chapter 2

# Pythagorean triangles

### 2.1 Construction of Pythagorean triangles

By a Pythagorean triangle we mean a right triangle whose side lengths are integers. Any common divisor of two of the side lengths is necessarily a divisor of the third. We shall call a Pythagorean triangle *primitive* if no two of its sides have a common divisor. Let  $(a, b, c)$  be one such triangle. From the relation  $a^2 + b^2 = c^2$ , we make the following observations.

1. Exactly two of  $a, b, c$  are odd, and the third is even.
2. In fact, the even number must be one of  $a$  and  $b$ . For if  $c$  is even, then  $a$  and  $b$  are both odd, and  $c^2 = a^2 + b^2 \equiv 1 + 1 = 2 \pmod{4}$ , an impossibility.
3. We shall assume  $a$  odd and  $b$  even, and rewrite the Pythagorean relation in the form

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

Note that the integers  $\frac{c+a}{2}$  and  $\frac{c-a}{2}$  are relatively prime, for any common divisor of these two numbers would be a common divisor  $c$  and  $a$ . Consequently, each of  $\frac{c+a}{2}$  and  $\frac{c-a}{2}$  is a square.

4. Writing  $\frac{c+a}{2} = u^2$  and  $\frac{c-a}{2} = v^2$ , we have  $c = u^2 + v^2$  and  $a = u^2 - v^2$ . From these,  $b = 2uv$ .
5. Since  $c$  and  $a$  are both odd,  $u$  and  $v$  are of different parity.

We summarize this in the following theorem.

**Theorem 2.1.** *The side lengths of a primitive Pythagorean triangle are of the form  $u^2 - v^2$ ,  $2uv$ , and  $u^2 + v^2$  for relatively prime integers  $u$  and  $v$  of different parity.*

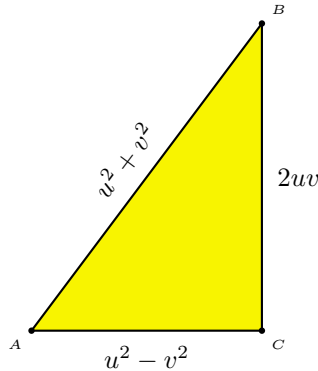


Figure 2.1: Primitive Pythagorean triangle

Here are some simple properties of a primitive Pythagorean triangle.

1. Exactly one leg is even.
2. Exactly one leg is divisible by 3.
3. Exactly one side is divisible by 5.
4. The area is divisible by 6.

#### Exercise

Three relatively prime numbers  $a$ ,  $b$ ,  $c$  are such that  $a^2$ ,  $b^2$ ,  $c^2$  are in arithmetic progression. Show that they can be written in the form

$$a = -p^2 + 2pq + q^2, \quad b = p^2 + q^2, \quad c = p^2 + 2pq - q^2$$

for relatively prime integers  $p$ ,  $q$  of different parity

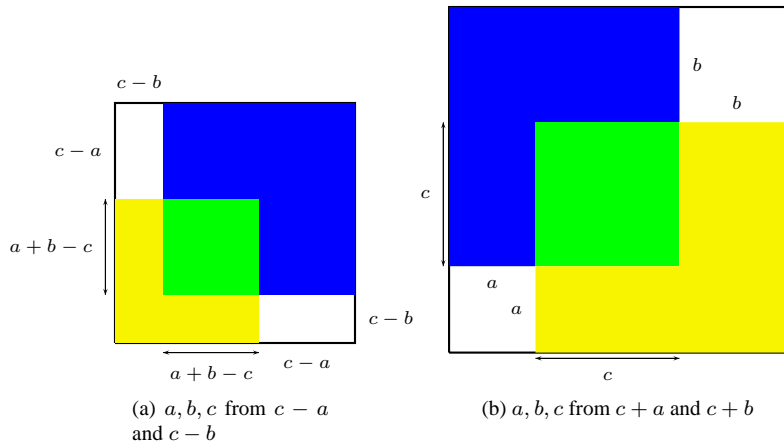
## 2.2 Primitive Pythagorean triangles with consecutive legs

Let  $a$ ,  $b$ ,  $c$  be the lengths of the sides of a right triangle,  $c$  the hypotenuse. Figures (a) and (b) below, together with the Pythagorean theorem, give

the following two relations

$$(a + b - c)^2 = 2(c - a)(c - b), \tag{2.1}$$

$$(a + b + c)^2 = 2(c + a)(c + b). \tag{2.2}$$



Beginning with a right triangle  $(a, b, c)$ , we construct a new right triangle  $(a', b', c')$  with  $c' - a' = c + b$  and  $c' - b' = c + a$ . By a comparison of (2.1) and (2.2), we have  $a' + b' - c' = a + b + c$ . From these,

$$\begin{aligned} a' &= 2a + b + 2c, \\ b' &= a + 2b + 2c, \\ c' &= 2a + 2b + 3c. \end{aligned}$$

Note that  $b' - a' = b - a$ . This construction therefore leads to an infinite sequence of integer right triangles with constant difference of legs. In particular, beginning with (3,4,5), we obtain the sequence

$$(3, 4, 5), (20, 21, 29), (119, 120, 169), (696, 697, 985), \dots$$

of Pythagorean triangles with legs differing by 1.

This construction gives *all* such Pythagorean triangles. Note that the above construction is invertible: from a right triangle  $(a', b', c')$  one can construct a *smaller* one  $(a, b, c)$  with the same difference between the

legs. More precisely,

$$\begin{aligned} a &= 2a' + b' - 2c', \\ b &= a' + 2b' - 2c', \\ c &= -2a' - 2b' + 3c'. \end{aligned} \tag{2.3}$$

Since  $a + b + c = a' + b' - c' < a' + b' + c'$ , this inverse construction does yield a smaller triangle. However, it certainly *cannot* lead to a strictly decreasing sequence of *integer* right triangles. Now,  $a = 2a' + b' - 2c'$  must be a positive integer. Using the Pythagorean theorem, it is easy to deduce from  $a' + b' > c'$  that  $4a' > 3b'$ , or  $a' > 3(b' - a')$ . This means that from every Pythagorean triangle with legs differing by 1, there is a descent, by repeated applications of (2.3), to a minimal integer right triangle with shortest side not exceeding 3. It is clear that there is only one such triangle, namely, (3,4,5). This therefore shows that the above construction actually gives *all* Pythagorean triangles with consecutive legs.

### 2.3 Fermat Last Theorem for $n = 4$

**Theorem 2.2 (Fermat).** *The area of a Pythagorean triangle cannot be a square.*

*Proof.* Suppose to the contrary there is one such triangle, which we may assume primitive, with side lengths  $(u^2 - v^2, 2uv, u^2 + v^2)$ ,  $u, v$  being relative prime of different parity. The area  $A = uv(u^2 - v^2)$  being a square, and no two of  $u, v, u^2 - v^2$  sharing common divisors, each of these numbers must be a square. We write  $u = a^2, v = b^2$  so that  $u^2 - v^2 = a^4 - b^4$  is also a square. Since  $a^4 - b^4 = (a^2 - b^2)(a^2 + b^2)$  and the two factors are relatively prime, we must have  $a^2 - b^2 = r^2$  and  $a^2 + b^2 = s^2$  for some integers  $r$  and  $s$ . From these,  $2a^2 = r^2 + s^2$  and

$$(2a)^2 = 2(r^2 + s^2) = (r + s)^2 + (r - s)^2.$$

Thus, we have a new Pythagorean triangle  $(r - s, r + s, 2a)$ . This is a Pythagorean triangle whose area is the square of an integer:

$$\frac{1}{2}(r - s)(r + s) = \frac{1}{2}(r^2 - s^2) = b^2.$$

But it is a *smaller* triangle since  $b^2 = v$  is a proper divisor of  $A = uv(u^2 - v^2)$ . By descent, beginning with one Pythagorean triangle with

square area, we obtain an infinite sequence of Pythagorean triangles with *decreasing* areas, each of which is a square integer; a contradiction.  $\square$

**Corollary 2.3 (Fermat Last Theorem for  $n = 4$ ).** *The equation*

$$x^4 + y^4 = z^4$$

*does not have solutions in nonzero integers.*

*Proof.* Suppose  $x^4 + y^4 = z^4$  for positive integers  $x, y, z$ . The Pythagorean triangle with sides  $z^4 - y^4, 2z^2y^2$  and  $z^4 + y^4$  has a square area

$$z^2y^2(z^4 - y^4) = z^2y^2x^4 = (x^2yz)^2,$$

a contradiction.  $\square$

*Remark.* This proof actually shows that the equation  $x^2 + y^4 = z^4$  has no solution in nonzero integers.

**Theorem 2.4.** *There is no integer right triangle whose area is twice a square.*

*Proof.* Suppose there is one such triangle, which we may assume primitive, with sides  $u^2 - v^2, 2uv, u^2 + v^2$  for relatively prime  $u$  and  $v$  of different parity. The area is  $uv(u^2 - v^2)$ . Note that  $u^2 - v^2$  and one of  $u, v$  must be odd. Since  $u^2 - v^2$  is an odd square,  $u$  is odd and  $v$  is even. The area being twice a square, we must have  $u = r^2, v = 2s^2, u + v = m^2, u - v = n^2$  for integers  $r, s, m, n$ .  $4s^2 = 2v = m^2 - n^2 = (m + n)(m - n)$ . Since  $m + n$  and  $m - n$  are even and have  $\gcd = 1$ , we have  $m + n = 2p^2$  and  $m - n = 2q^2$  for relatively prime integers  $p$  and  $q$ . Thus,  $m = p^2 + q^2$  and  $n = p^2 - q^2$ . Also,

$$p^4 + q^4 = \frac{1}{2}((p^2 + q^2)^2 + (p^2 - q^2)^2) = \frac{1}{2}(m^2 + n^2) = u = r^2.$$

This gives a smaller integer triangle of sides  $(p^2, q^2, r)$  whose area is  $\frac{1}{2}(p^2q^2) = 2\left(\frac{pq}{2}\right)^2$ , twice a square. By descent, we arrive at a contradiction.  $\square$

**Corollary 2.5.** *The equation  $x^4 + y^4 = z^2$  has no nontrivial solution in positive integers.*<sup>1</sup>

<sup>1</sup>Here is a more direct proof of the corollary without invoking Pythagorean triangles. Suppose  $x^4 + y^4 = z^2$  with  $x, y, z$  pairwise relatively prime. By considering the equation modulo 4, we see that  $z$  and exactly one of  $x, y$  must be odd. Assume  $x$  even. Note that  $x^4 = z^2 - y^4 = (z - y^2)(z + y^2)$ . The two factors

**Corollary 2.6.** *The product of 4 nonzero integers in arithmetic progression (with nonzero common difference) cannot be a fourth power of an integer.*

*Proof.* Given four integers in A. P., by doubling if necessary, we may write the numbers as  $a - 3d$ ,  $a - d$ ,  $a + d$ , and  $a + 3d$ , for integers  $a$  and  $d$ . If their product

$$(a - 3d)(a - d)(a + d)(a + 3d) = (a^2 - d^2)(a^2 - 9d^2) = a^4 - 10a^2d^2 + 9d^4$$

is a fourth power, say  $x^4$ , we have  $x^4 + (2d)^4 = (a^2 - 5d^2)^2$ , an impossibility since  $d$  and  $x$  are nonzero.  $\square$

*Remark.* We shall later prove the stronger result that the product of 4 distinct nonzero integers in arithmetic progression cannot be a square.

### Exercise

Prove that the product of 4 consecutive integers cannot be a square.

## 2.4 Nonexistence of a pair of Pythagorean triangles with legs $a$ , $b$ , and $a$ , $2b$

**Proposition 2.7.** *There do not exist a pair of integer right triangles with legs  $(a, b)$  and  $(a, 2b)$ .*

*Proof.* Suppose there is one such pair. We may assume  $a$ ,  $b$  relatively prime. We may also assume  $a$  odd, for if  $a$  is even, then we may replace by the smaller pair  $(\frac{a}{2}, b)$  and  $(a, b)$ . There are integers  $u$ ,  $v$ ,  $x$ ,  $y$  such that

(i)  $u$  and  $v$  are relatively prime and of different parity, and

$$a = u^2 - v^2, \quad b = 2uv;$$

(ii)  $x$  and  $y$  are relatively prime and of different parity, and

$$a = x^2 - y^2, \quad b = xy.$$

$z - y^2$  and  $z + y^2$  are both even; yet they cannot be both divisible by 4. We have two possibilities:

(i)  $z + y^2 = 8u^4$  and  $z - y^2 = 2v^4$  for relatively prime  $u$  and  $v$ , or

(ii)  $z + y^2 = 2u^4$  and  $z - y^2 = 8v^4$ .

In (i),  $y^2 = 4u^4 - v^4$ . But this is a contradiction modulo 4. Therefore, we must have (ii) and  $y^2 = u^4 - 4v^4$ . Thus,  $(u^2 + y)(u^2 - y) = 4v^4$ . Thus,  $u$  and  $y$  are both odd, and  $u^2 + y = 2r^4$  and  $u^2 - y = 2s^4$  for relatively prime  $r$  and  $s$ . From this,  $r^4 + s^4 = u^2$ . This is a smaller solution of the same equation since  $z = u^4 + 4v^4 > u$ . By infinite descent, the equation has no nontrivial solution in positive integers.

This means  $xy = 2uv$ . There exist pairwise relatively prime integers  $p, q, r, s$  such that

$$x = pq, \quad y = 2rs; \quad u = pr, \quad v = qs.$$

Substitution into  $x^2 - y^2 = u^2 - v^2$  gives

$$q^2(p^2 + s^2) = r^2(p^2 + 4s^2).$$

Now,  $q$  is prime to  $r$  and  $p$  is prime to  $s$ . Note that any common divisor of  $p^2 + s^2$  and  $p^2 + 4s^2$  must divide their difference and hence must be a multiple of 3. This is impossible since  $\gcd(p, s) = 1$ .<sup>2</sup> It follows that  $p^2 + s^2 = r^2$  and  $p^2 + 4s^2 = q^2$ , and we have a smaller pair of integer right triangles with legs  $(p, s)$  and  $(p, 2s)$ . This pair is indeed smaller since  $s \leq v < b$ . This is a contradiction by infinite descent.  $\square$

Therefore, it is impossible to make  $x^2 + y^2$  and  $x^2 + 4y^2$  simultaneously squares. This is often expressed by saying that the two quadratic forms are *discordant*.

## 2.5 Impossibility of 4 squares in arithmetic progression

We study the possibility of four integer squares in arithmetic progression. It is well known that  $n^2$  is the sum of the first  $n$  odd numbers, *i.e.*,

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

Suppose four integer squares  $A^2, B^2, C^2, D^2$  are in arithmetic progression. This means that the three segments of consecutive odd numbers

$$\begin{aligned} &2A + 1, \dots, 2B - 1, \\ &2B + 1, \dots, 2C - 1, \\ &2C + 1, \dots, 2D - 1 \end{aligned}$$

have equal sums. These segments have  $a = B - A, b = C - B$ , and  $c = D - C$  numbers respectively. Their sums are

$$\begin{aligned} a(A + B) &= a(2B - a), \\ b(B + C) &= b(2B + b) = b(2C - b), \\ c(C + D) &= c(2C + c). \end{aligned}$$

---

<sup>2</sup> $p^2 + s^2 \equiv 0 \pmod{3}$  only if  $p \equiv s \equiv 0 \pmod{3}$ .

The first two have equal sums if and only if  $2B = \frac{a^2+b^2}{a-b}$ . Likewise, the last two have equal sums if and only if  $2C = \frac{b^2+c^2}{b-c}$ . It follows that if the three sums are equal, then  $\frac{b^2+c^2}{b-c} - \frac{a^2+b^2}{a-b} = 2b$ . Simplifying this, we have

$$(a+c)b^2 + (a-c)^2b - ac(a+c) = 0.$$

This has integer solution in  $b$  only if  $(a-c)^4 + 4ac(a+c)^2 = a^4 + 14a^2c^2 + c^4$  is the square of an integer. By writing  $x = a+c$  and  $y = a-c$ , we have  $x^4 - x^2y^2 + y^4 = z^2$  for some integer  $z$ .

**Proposition 2.8.** *The Diophantine equation  $x^4 - x^2y^2 + y^4 = z^2$  has no nonzero solutions in integers except  $x^2 = y^2 = z^2$ .*

*Proof.* Suppose there is a positive integer solution with  $x > y$ . We may assume  $x$  and  $y$  relatively prime, and rewrite the equation in the form

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

Here,  $x^2 - y^2$  and  $xy$  are relatively prime, so that  $(x^2 - y^2, xy, z)$  is a primitive Pythagorean triple.

(1) Suppose both  $x$  and  $y$  are odd. Then there are relatively prime  $u, v$ , of different parity, so that

$$x^2 - y^2 = 2uv, \quad xy = u^2 - v^2.$$

Here,

$$(u^2 - v^2)^2 + (uv)^2 = \left(\frac{x^2 + y^2}{2}\right)^2,$$

or

$$u^4 - u^2v^2 + v^4 = z'^2,$$

This is an equation of the same type, in which  $u$  and  $v$  have different parity. It is a smaller solution since

$$\begin{aligned} z'^2 &= \left(\frac{x^2 + y^2}{2}\right)^2 = \frac{1}{4}[(x^2 - y^2)^2 + 4(xy)^2] \\ &= u^2v^2 + (u^2 - v^2)^2 < (u^2 + v^2)^2 = z^2. \end{aligned}$$

(2) Now consider the case when  $x$  and  $y$  are of different parity. We shall assume  $y$  even. There are relatively prime integers  $u$  and  $v$  such that

$$x^2 - y^2 = u^2 - v^2, \quad xy = 2uv.$$

This gives a pair of integer right triangles with legs  $(a, b)$  and  $(a, 2b)$ . Such a pair does not exist by Proposition 2.7.  $\square$

**Theorem 2.9.** *There do not exist 4 distinct nonzero squares in arithmetical progression.*

**Theorem 2.10.** *The product of 4 nonzero integers in arithmetic progression (with nonzero common difference) cannot be a square.*

*Proof.* Consider an arithmetic progression  $a, a + d, a + 2d, a + 3d$  of integers with a square product. We may assume  $\gcd(a, d) = 1$ . The only possibility of a pair of these numbers admitting a common divisor are

(i)  $\gcd(a, a + 2d) = 2$ ,

(ii)  $\gcd(a + d, a + 3d) = 2$ , or

(iii)  $\gcd(a, a + 3d) = 3$ . Therefore, each of the numbers  $a, a + d, a + 2d, a + 3d$  is a square with a possibly extra factor 2, 3 or 6. Here are the only possibilities:

(a)  $A^2, B^2, C^2, D^2$ ;

(b)  $6A^2, B^2, 2C^2, 3D^2$ ;

(c)  $3A^2, 2B^2, C^2, 6D^2$ .

Case (a) is impossible by Theorem 2.9.

For cases (b) and (c), we make use of the easily verified identity (for four terms in arithmetic progression):

$$(a + 2d)(a + 3d) - a(a + d) = 2((a + d)(a + 3d) - a(a + 2d)).$$

In (b), we have  $(2C^2)(3D^2) - (6A^2)(B^2) = 2((B^2)(3D^2) - (6A^2)(2C^2))$ , and  $C^2(4A^2 + D^2) = B^2(A^2 + D^2)$ . Since we may assume  $A, B, C, D$  relatively prime, this means that  $A^2 + D^2$  and  $4A^2 + D^2$  are both squares, contradicting Proposition 2.7

Similarly, in (c), we have  $C^2(A^2 + D^2) = B^2(A^2 + 4D^2)$ , a contradiction for the same reasoning.  $\square$

## Appendix: Primitive Pythagorean triples &lt; 1000

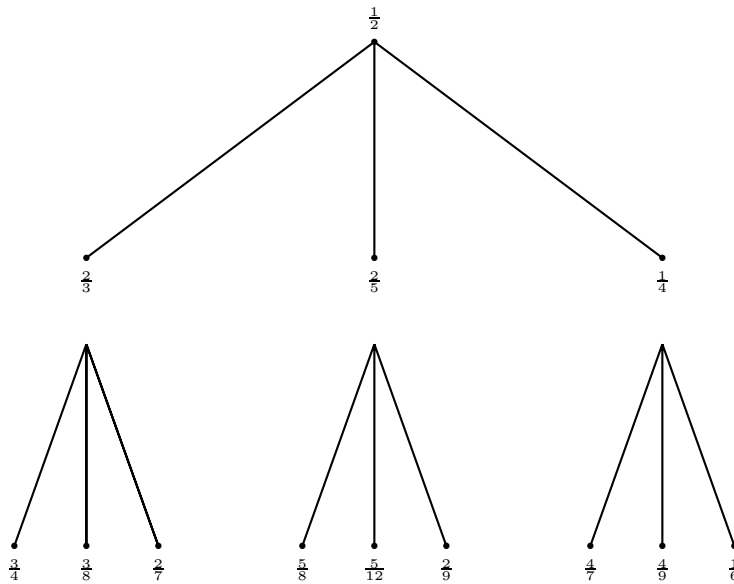
$m, n$	$a, b, c$	$m, n$	$a, b, c$	$m, n$	$a, b, c$	$m, n$	$a, b, c$
2, 1	3, 4, 5	3, 2	5, 12, 13	4, 1	15, 8, 17	4, 3	7, 24, 25
5, 2	21, 20, 29	5, 4	9, 40, 41	6, 1	35, 12, 37	6, 5	11, 60, 61
7, 2	45, 28, 53	7, 4	33, 56, 65	7, 6	13, 84, 85	8, 1	63, 16, 65
8, 3	55, 48, 73	8, 5	39, 80, 89	8, 7	15, 112, 113	9, 2	77, 36, 85
9, 4	65, 72, 97	9, 8	17, 144, 145	10, 1	99, 20, 101	10, 3	91, 60, 109
10, 7	51, 140, 149	10, 9	19, 180, 181	11, 2	117, 44, 125	11, 4	105, 88, 137
11, 6	85, 132, 157	11, 8	57, 176, 185	11, 10	21, 220, 221	12, 1	143, 24, 145
12, 5	119, 120, 169	12, 7	95, 168, 193	12, 11	23, 264, 265	13, 2	165, 52, 173
13, 4	153, 104, 185	13, 6	133, 156, 205	13, 8	105, 208, 233	13, 10	69, 260, 269
13, 12	25, 312, 313	14, 1	195, 28, 197	14, 3	187, 84, 205	14, 5	171, 140, 221
14, 9	115, 252, 277	14, 11	75, 308, 317	14, 13	27, 364, 365	15, 2	221, 60, 229
15, 4	209, 120, 241	15, 8	161, 240, 289	15, 14	29, 420, 421	16, 1	255, 32, 257
16, 3	247, 96, 265	16, 5	231, 160, 281	16, 7	207, 224, 305	16, 9	175, 288, 337
16, 11	135, 352, 377	16, 13	87, 416, 425	16, 15	31, 480, 481	17, 2	285, 68, 293
17, 4	273, 136, 305	17, 6	253, 204, 325	17, 8	225, 272, 353	17, 10	189, 340, 389
17, 12	145, 408, 433	17, 14	93, 476, 485	17, 16	33, 544, 545	18, 1	323, 36, 325
18, 5	299, 180, 349	18, 7	275, 252, 373	18, 11	203, 396, 445	18, 13	155, 468, 493
18, 17	35, 612, 613	19, 2	357, 76, 365	19, 4	345, 152, 377	19, 6	325, 228, 397
19, 8	297, 304, 425	19, 10	261, 380, 461	19, 12	217, 456, 505	19, 14	165, 532, 557
19, 16	105, 608, 617	19, 18	37, 684, 685	20, 1	399, 40, 401	20, 3	391, 120, 409
20, 7	351, 280, 449	20, 9	319, 360, 481	20, 11	279, 440, 521	20, 13	231, 520, 569
20, 17	111, 680, 689	20, 19	39, 760, 761	21, 2	437, 84, 445	21, 4	425, 168, 457
21, 8	377, 336, 505	21, 10	341, 420, 541	21, 16	185, 672, 697	21, 20	41, 840, 841
22, 1	483, 44, 485	22, 3	475, 132, 493	22, 5	459, 220, 509	22, 7	435, 308, 533
22, 9	403, 396, 565	22, 13	315, 572, 653	22, 15	259, 660, 709	22, 17	195, 748, 773
22, 19	123, 836, 845	22, 21	43, 924, 925	23, 2	525, 92, 533	23, 4	513, 184, 545
23, 6	493, 276, 565	23, 8	465, 368, 593	23, 10	429, 460, 629	23, 12	385, 552, 673
23, 14	333, 644, 725	23, 16	273, 736, 785	23, 18	205, 828, 853	23, 20	129, 920, 929
24, 1	575, 48, 577	24, 5	551, 240, 601	24, 7	527, 336, 625	24, 11	455, 528, 697
24, 13	407, 624, 745	24, 17	287, 816, 865	24, 19	215, 912, 937	25, 2	621, 100, 629
25, 4	609, 200, 641	25, 6	589, 300, 661	25, 8	561, 400, 689	25, 12	481, 600, 769
25, 14	429, 700, 821	25, 16	369, 800, 881	25, 18	301, 900, 949	26, 1	675, 52, 677
26, 3	667, 156, 685	26, 5	651, 260, 701	26, 7	627, 364, 725	26, 9	595, 468, 757
26, 11	555, 572, 797	26, 15	451, 780, 901	26, 17	387, 884, 965	27, 2	725, 108, 733
27, 4	713, 216, 745	27, 8	665, 432, 793	27, 10	629, 540, 829	27, 14	533, 756, 925
27, 16	473, 864, 985	28, 1	783, 56, 785	28, 3	775, 168, 793	28, 5	759, 280, 809
28, 9	703, 504, 865	28, 11	663, 616, 905	28, 13	615, 728, 953	29, 2	837, 116, 845
29, 4	825, 232, 857	29, 6	805, 348, 877	29, 8	777, 464, 905	29, 10	741, 580, 941
29, 12	697, 696, 985	30, 1	899, 60, 901	30, 7	851, 420, 949	31, 2	957, 124, 965
31, 4	945, 248, 977	31, 6	925, 372, 997				

## 5.7. Genealogy of primitive Pythagorean triples

A. Hall [6] has arranged the totality the primitive Pythagorean triples in the form of a binary tree, with the  $(3, 4, 5)$  triangle at its root. Recall that a primitive Pythagorean triangle is represented by a unique rational number  $t = \frac{n}{m}$ , with  $\gcd(m, n) = 1$  and  $m, n$  of different parity. We call

$t$  the rational parameter of the primitive Pythagorean triangle.

In this genealogy, each primitive Pythagorean triangle (with parameter  $t$ ) has exactly three descendents, with rational parameters  $s = \frac{1}{2-t}, \frac{1}{2+t}, \frac{t}{1+2t}$  respectively. (Check that each of these rational parameters does lie in the open interval  $(0, 1)$ , and is represented by a reduced fraction whose numerator and denominator are of different parity). We shall keep to this order of the descendents and label them the left (L), middle (M), and right (R) respectively. Thus, the  $(3, 4, 5)$  triangle, with rational parameter  $\frac{1}{2}$  has left descendent  $\frac{2}{3}$ , middle descendent  $\frac{2}{5}$  and right descendent  $\frac{1}{4}$ .



If we write  $t = \frac{n}{m}$ , then these three descendents are  $\frac{m}{2m-n}, \frac{m}{2m+n}$  and  $\frac{n}{m+2n}$ . If we call  $n + m$  the heights of the rational number  $\frac{n}{m}$  in reduced form, these three descendents have greater heights.

Now, each rational number  $s \in (0, 1) \setminus \{\frac{1}{3}, \frac{1}{2}\}$  is the descendent of a unique rational number  $t$ . In fact, given a rational number  $s = \frac{q}{p} \in (0, 1)$ , **exactly one** of  $\frac{2s-1}{s} = \frac{2q-p}{q}, \frac{1-2s}{s} = \frac{p-2q}{q}$ , and  $\frac{s}{1-2s} = \frac{q}{p-2q}$  is in  $(0, 1)$ . We call this the *parent* of  $s$ . In fact,  $s$  is

- (i) the left descendent of  $\frac{2q-p}{q}$  if  $q < p < 2q$ ,
- (ii) the middle descendent of  $\frac{p-2q}{q}$  if  $2q < p < 3q$ , and
- (iii) the right descendent of  $\frac{q}{p-2q}$  if  $p > 3q$ .

Therefore, each rational parameter  $s \in (0, 1) \setminus \{\frac{1}{3}, \frac{1}{2}\}$  has a unique “ancestral sequence” tracing back to the root  $\frac{1}{2}$  (of height 3). For example,

$$\frac{23}{36} \xleftarrow{L} \frac{10}{23} \xleftarrow{M} \frac{3}{10} \xleftarrow{R} \frac{3}{4} \xleftarrow{L} \frac{2}{3} \xleftarrow{L} \frac{1}{2}.$$

If we “flatten” the entire ternary tree by listing the vertices in order, beginning with the “root”, going down through each level from left to right, what is the position of a vertex with a known ancestral sequence? Suppose this ancestral sequence has  $k$  terms, *i.e.*, the vertex is  $k$  levels below the root. Convert it into an integer  $N$  in base 3 expansion by

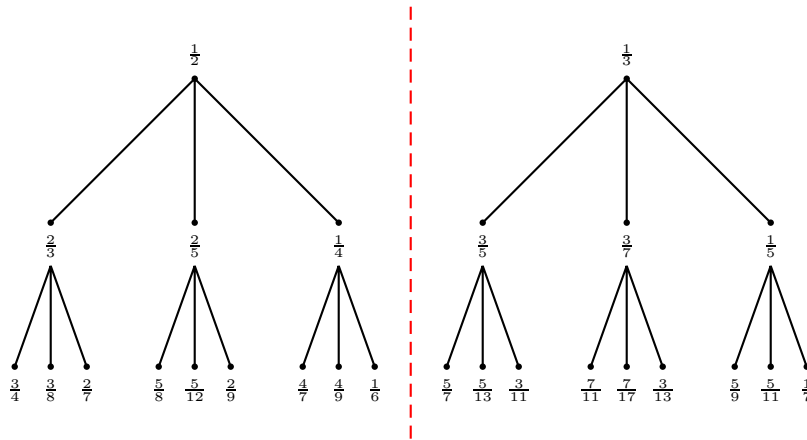
$$L \rightarrow 0, \quad M \rightarrow 1, \quad R \rightarrow 2$$

respectively. Then the position of the vertex in the list is  $\frac{1}{2}(3^k + 1) + N$ . For example, the rational number  $\frac{23}{36}$  is in position  $\frac{1}{2}(3^5 + 1) + 01200_3 = 122 + 45 = 167$ .

### Exercise

What is the 1000-th vertex in this list?  $1000 = 1 + 1 + 3 + 3^2 + 3^3 + 3^4 + 3^5 + 635$ . The base 3 expansion of 635 is  $212112_3$ . The ancestral sequence of the vertex is therefore

$$\frac{40}{169} \xleftarrow{R} \frac{40}{89} \xleftarrow{M} \frac{9}{40} \xleftarrow{R} \frac{9}{22} \xleftarrow{M} \frac{4}{9} \xleftarrow{M} \frac{1}{4} \xleftarrow{R} \frac{1}{2}.$$



## Chapter 3

# Homogeneous quadratic equations in 3 variables

### 3.1 Pythagorean triangles revisited

A primitive Pythagorean triangle  $(a, b, c)$  corresponds to a point  $(x, y) = \left(\frac{a}{c}, \frac{b}{c}\right)$  in the first quadrant on the unit circle

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

Every rational point on the unit circle can be expressed in terms of the slope of the line joining the point to a fixed point, say  $P = (-1, 0)$  on the circle. Thus, solving the equations

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

simultaneously, we obtain  $(x, y) = (-1, 0) = P$  or

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

This is a point in the first quadrant if and only if  $0 < t < 1$ . By putting  $t = \frac{q}{p}$  for relatively prime integers  $p > q$ , and we obtain  $\left(\frac{p^2 - q^2}{p^2 + q^2}, \frac{2pq}{p^2 + q^2}\right)$ . It follows that the sidelengths of a primitive Pythagorean triangle can be written in the form

$$(a, b, c) = \frac{1}{g} (p^2 - q^2, 2pq, p^2 + q^2)$$

for suitable choice of  $p$  and  $q$ . Here,

$$g = \gcd(p^2 - q^2, 2pq) = \gcd(p^2 - q^2, 2) = \gcd(p - q, 2).$$

To avoid repetition of representing a primitive Pythagorean triangle by both  $(x, y)$  and  $(y, x)$  in the first quadrant, we note that  $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) = \left(\frac{2s}{1+s^2}, \frac{1-s^2}{1+s^2}\right)$  if and only if  $s = \frac{1-t}{1+t}$ . Thus, the rational number  $t = \frac{q}{p}$  and  $s = \frac{q'}{p'} = \frac{p-q}{p+q}$  represent the same primitive Pythagorean triangle. Note that  $\gcd(p - q, 2) = 1$  if and only if  $\gcd(p' - q', 2) = 2$ . Thus, we may always restrict  $p$  and  $q$  of different parity.

### 3.2 Rational points on a conic

The method in the preceding section applies to a general (nonsingular) homogeneous equation in 3 variables, or after dehomogenization, to a nonsingular conic in the Cartesian plane. Suppose a nonsingular conic  $f(x, y) = c$  contains a rational point  $P = (x_0, y_0)$ . Then by passing through  $P$  lines of rational slope  $t$  to intersect the conic again, we obtain a parametrization of the rational points on the curve.

**Proposition 3.1.** (1) *The rational solutions of  $x^2 - dy^2 = 1$  can be parametrized in the form*

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

(2) *The positive integer solutions of  $x^2 - dy^2 = z^2$  can be parametrized in the form*

$$(x, y, z) = \frac{1}{g} (p^2 + dq^2, 2pq, p^2 - dq^2),$$

where  $g = \gcd(p^2 + dq^2, 2pq, p^2 - dq^2)$ .

## Chapter 4

# Integer triangles with a $60^\circ$ or $120^\circ$ angle

### 4.1 Integer triangles with a $60^\circ$ angle

If triangle  $ABC$  has  $C = 60^\circ$ , then

$$c^2 = a^2 - ab + b^2. \quad (4.1)$$

Integer triangles with a  $60^\circ$  angle therefore correspond to rational points in the first quadrant on the curve

$$x^2 - xy + y^2 = 1. \quad (4.2)$$

Note that the curve contains the point  $P = (-1, -1)$ . By passing a line of rational slope  $t$  through  $P$  to intersect the curve again, we obtain a parametrization of the rational points. Now, such a line has equation  $y = -1 + t(x + 1)$ . Solving this simultaneously with (4.2) we obtain  $(x, y) = (-1, -1) = P$ , and

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

which is in the first quadrant if  $\frac{1}{2} < t \leq 2$ . By symmetry, we may simply take  $\frac{1}{2} < t \leq 1$  to avoid repetition. Putting  $t = \frac{q}{p}$  for relatively prime integers  $p, q$ , and clearing denominators, we obtain

$$\begin{aligned} a &= p(2q - p), \\ b &= q(2p - q), \\ c &= p^2 - pq + q^2, \end{aligned}$$

with  $\frac{p}{2} < q \leq p$ .

$$\begin{aligned} \gcd(a, b) &= \gcd(2pq - p^2, 2pq - q^2) \\ &= \gcd((p - q)(p + q), q(2p - q)) \\ &= \gcd((p - q)(p + q), 2p - q) \end{aligned}$$

since  $\gcd(p - q, q) = \gcd(p + q, q) = \gcd(p, q) = 1$ . Now,  
 $\gcd(p - q, 2p - q) = \gcd(p - q, p) = 1$  and  
 $\gcd(p + q, 2p - q) = \gcd(p + q, 3p) = \gcd(p + q, 3)$ . This gives  
 $\gcd(a, b) = \gcd(p + q, 3)$ .

**Proposition 4.1.** *The primitive integer triangles with a  $60^\circ$  angle are given by*

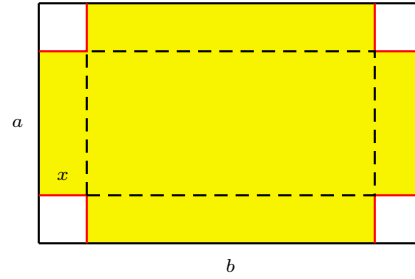
$$\frac{1}{g} (p(2q - p), q(2p - q), p^2 - pq + q^2),$$

where  $p$  and  $q$  are relatively prime positive integers satisfying  $\frac{p}{2} < q \leq p$  and  $g = \gcd(p + q, 3)$ .

$p$	$q$	$(a, b, c)$
1	1	(1, 1, 1)
3	2	(3, 8, 7)
4	3	(8, 15, 13)
5	3	(5, 21, 19)
5	4	(5, 8, 7)
6	5	(24, 35, 31)
7	4	(7, 40, 37)
7	5	(7, 15, 13)
7	6	(35, 48, 43)
8	5	(16, 55, 49)
8	7	(16, 21, 19)
9	5	(9, 65, 61)
9	7	(45, 77, 67)
9	8	(63, 80, 73)
10	7	(40, 91, 79)
10	9	(80, 99, 91)

### Exercise

A standard calculus exercise asks to cut equal squares of dimension  $x$  from the four corners of a rectangle of length  $a$  and breadth  $b$  so that the box obtained by folding along the creases has a greatest capacity.



The answer to this problem is given by

$$x = \frac{a + b - \sqrt{a^2 - ab + b^2}}{6}.$$

How should one choose relatively prime integers  $a$  and  $b$  so that the resulting  $x$  is an integer? For example, when  $a = 5$ ,  $b = 8$ ,  $x = 1$ . Another example is  $a = 16$ ,  $b = 21$  with  $x = 3$ .

## 4.2 Integer triangles with a $120^\circ$ angle

If triangle  $ABC$  has  $C = 120^\circ$ , then

$$c^2 = a^2 + ab + b^2. \quad (4.3)$$

Integer triangles with a  $120^\circ$  angle therefore correspond to rational points in the first quadrant on the curve

$$x^2 + xy + y^2 = 1. \quad (4.4)$$

Note that the curve contains the point  $Q = (-1, 0)$ . By passing a line of rational slope  $t$  through  $P$  to intersect the curve again, we obtain a parametrization of the rational points. Now, such a line has equation  $y = t(x + 1)$ . Solving this simultaneously with (4.2) we obtain  $(x, y) = (-1, 0) = Q$ , and

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

which is in the first quadrant if  $0 < t < 1$ . It is easy to check that  $Q(t)$  and  $Q\left(\frac{1-t}{1+2t}\right)$  are symmetric about the line  $y = x$ . To avoid repetition we may restrict to  $0 < t < \frac{\sqrt{3}-1}{2}$ .

Putting  $t = \frac{q}{p}$  for relatively prime integers  $p, q$  satisfying  $q < \frac{\sqrt{3}-1}{2}p$ , and clearing denominators, we obtain

$$\begin{aligned} a &= p^2 - q^2, \\ b &= q(2p + q), \\ c &= p^2 + pq + q^2, \end{aligned}$$

with  $0 < q < p$ . Note that

$$\begin{aligned} \gcd(p^2 - q^2, q(2p + q)) &= \gcd((p + q)(p - q), q(2p + q)) \\ &= \gcd((p + q)(p - q), 2p + q) \\ &= \gcd(p - q, 2p + q) \\ &= \gcd(p - q, 3p) \\ &= \gcd(p - q, 3). \end{aligned}$$

**Proposition 4.2.** *The primitive integer triangles with a  $120^\circ$  angle are given by*

$$\frac{1}{g} (p^2 - q^2, q(2p + q), p^2 + pq + q^2),$$

where  $q < \left(\frac{\sqrt{3}-1}{2}\right)p$  are relatively prime positive integers and  $g = \gcd(p - q, 3)$ .

$p$	$q$	$(a, b, c)$
3	1	(8, 7, 13)
4	1	(5, 3, 7)
5	1	(24, 11, 31)
6	1	(35, 13, 43)
7	1	(16, 5, 19)
7	2	(45, 32, 67)
8	1	(63, 17, 73)
9	1	(80, 19, 91)
9	2	(77, 40, 103)
10	1	(33, 7, 37)
10	3	(91, 69, 139)

### Exercise

1 (a) Show that a number  $c$  is a sum of two consecutive squares if and only if  $2c - 1$  is a square.

(b) Suppose an integer triangle contains a  $120^\circ$  angle with its two arms differing by 1. Show that the length of the longest side is a sum of two consecutive squares.

2. It is known that the centroid of a triangle of sides  $a, b, c$  lies on its incircle if and only if

$$5(a^2 + b^2 + c^2) = 6(ab + bc + ca).$$

Find a parametrization of all such primitive triangles.

### 4.3 A pair of discordant forms: $x^2 \pm xy + y^2$

We show that it is impossible to have a pair of integer triangles with the same adjacent sides  $x, y$  and included angles equal to  $60^\circ$  and  $120^\circ$  respectively. In other words,  $x^2 - xy + y^2$  and  $x^2 + xy + y^2$  cannot be made squares simultaneously. If so, then their product would be a square, namely,  $x^4 + x^2y^2 + y^4 = \square$ . This contradicts the following theorem.

**Proposition 4.3.** *There do not exist a pair of Pythagorean triangles of sidelengths  $(a, b, c)$  and  $(a', 2b, c)$ .*

The proof is similar to Proposition 2.7.

**Theorem 4.4.** *The Diophantine equation  $x^4 + x^2y^2 + y^4 = z^2$  does not have nonzero solutions in integers.*

*Proof.* Suppose the equation has nontrivial solutions in integers  $x, y, z$ , which we may assume relatively prime. Then  $(x^2 + y^2)^2 = z^2 + (xy)^2$ . This gives a primitive Pythagorean triangle, say with parameters  $u$  and  $v$ . This means  $x$  and  $y$  are of different parity, and  $xy = 2uv$ ,  $z = u^2 - v^2$ . This gives a pair of Pythagorean triangles with equal hypotenuses and one with a leg twice a leg of the other, and is a contradiction to Proposition 4.3.  $\square$

#### Exercise

Show that in a parallelogram with a  $60^\circ$  angle, the side and the diagonals cannot all have integer lengths.



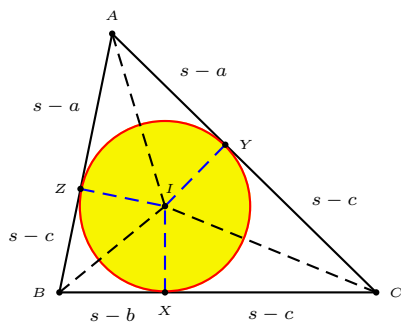
## Chapter 5

# Heron triangles

### 5.1 The Heron formula

Let  $ABC$  be a triangle with sidelengths  $BC = a$ ,  $CA = b$ ,  $AB = c$ , and semiperimeter  $s = \frac{1}{2}(a + b + c)$ . If the incircle touches the sides  $BC$ ,  $CA$  and  $AB$  respectively at  $X$ ,  $Y$ , and  $Z$ ,

$$AY = AZ = s - a, \quad BX = BZ = s - b, \quad CX = CY = s - c.$$



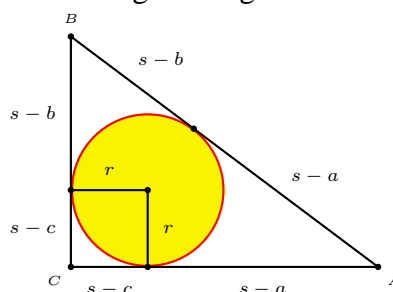
The radius  $r$  of the incircle and the area  $\Delta$  of the triangle are given by

$$r = \sqrt{\frac{(s-a)(s-b)(s-c)}{s}},$$
$$\Delta = \sqrt{s(s-a)(s-b)(s-c)}.$$

The latter one is the famous Heron formula. Explicitly in terms of  $a$ ,  $b$ ,  $c$ , it can be written as

$$\Delta^2 = \frac{1}{16} (2a^2b^2 + 2b^2c^2 + 2c^2a^2 - a^4 - b^4 - c^4). \quad (5.1)$$

*Remark.* The inradius of a right triangle is  $r = s - c$ .



### Exercise

Given a positive integer  $r$ , determine all Pythagorean triangles with inradius  $r$ .

First consider the case of primitive Pythagorean triangles. The one with parameters  $p > q$  (of different parity) has inradius  $r = q(p - q)$ . Note that  $p - q$  must be odd, and  $q$  does not contain any prime divisor of  $p - q$ . There are  $2^k$  choices of  $p - q$ , where  $k$  is the number of *odd* prime divisors of  $r$ . In particular, there is only one (primitive) Pythagorean triangle of inradius 1, which is the (3, 4, 5) triangle.

## 5.2 Heron triangles

A Heron triangle is an integer triangle with integer area. Here are some fundamental facts about Heron triangles.

**Proposition 5.1.** (1) *The semiperimeter of a Heron triangle is an integer.*  
 (2) *The area of a Heron triangle is a multiple of 6.*

*Proof.* It is enough to consider primitive Heron triangles, those whose sides are relatively prime.

(1) Note that modulo 16, each of  $a^4, b^4, c^4$  is congruent to 0 or 1, according as the number is even or odd. To render in (5.1) the sum  $2a^2b^2 + 2b^2c^2 + 2c^2a^2 - a^4 - b^4 - c^4 \equiv 0$  modulo 16, exactly two of  $a, b, c$  must be odd. It follows that the perimeter of a Heron triangle must be an even number.

(2) Since  $a, b, c$  are not all odd nor all even, and  $s$  is an integer, at least one of  $s - a, s - b, s - c$  is even. This means that  $\Delta$  is even. We claim that at least one of  $s, s - a, s - b, s - c$  must be a multiple of 3. If not, then modulo 3, these numbers are  $+1$  or  $-1$ . Since  $s = (s - a) + (s - b) + (s - c)$ , modulo 3, this must be either  $1 \equiv 1 + 1 + (-1)$  or

$-1 \equiv 1 + (-1) + (-1)$ . In each case the product  $s(s-a)(s-b)(s-c) \equiv -1 \pmod{3}$  cannot be a square. This justifies the claim that one of  $s, s-a, s-b, s-c$ , hence  $\triangle$ , must be a multiple of 3.  $\square$

### 5.3 Construction of Heron triangles

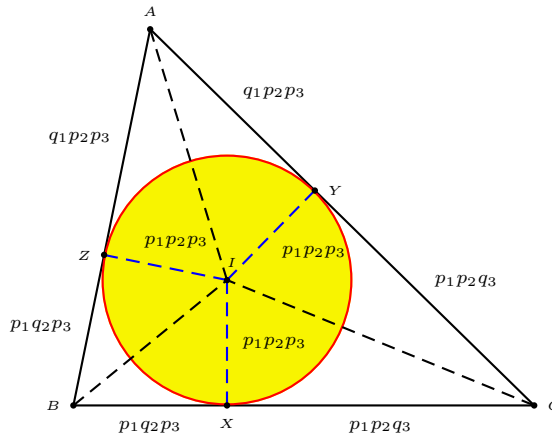
Let  $t_1 = \tan \frac{A}{2}$ ,  $t_2 = \tan \frac{B}{2}$ , and  $t_3 = \tan \frac{C}{2}$ . Since  $\frac{A}{2} + \frac{B}{2} + \frac{C}{2} = \frac{\pi}{2}$ , we have  $t_1 t_2 + t_2 t_3 + t_3 t_1 = 1$ . If we construct a triangle with sides  $\frac{1}{t_2} + \frac{1}{t_3}$ ,  $\frac{1}{t_3} + \frac{1}{t_1}$ , and  $\frac{1}{t_1} + \frac{1}{t_2}$ , then it has inradius 1 and area

$$\sqrt{\frac{1}{t_1} \cdot \frac{1}{t_2} \cdot \frac{1}{t_3} \left( \frac{1}{t_1} + \frac{1}{t_2} + \frac{1}{t_3} \right)} = \frac{1}{t_1 t_2 t_3}.$$

Writing  $t_i = \frac{p_i}{q_i}$  for relatively prime integers  $p_i, q_i, i = 1, 2$ , and magnifying the triangle by a factor  $p_1 p_2 p_3$ , we obtain a Heron triangle with sides

$$a = p_1(p_2 q_3 + p_3 q_2), \quad b = p_2(p_3 q_1 + p_1 q_3), \quad c = p_3(p_1 q_2 + p_2 q_1),$$

and area  $p_1 p_2 p_3 q_1 q_2 q_3$  and inradius  $p_1 p_2 p_3$ .



Note that these integers satisfy

$$p_1 p_2 q_3 + p_1 q_2 p_3 + q_1 p_2 p_3 = q_1 q_2 q_3,$$

or

$$\frac{p_3}{q_3} = \frac{q_1 q_2 - p_1 p_2}{p_1 q_2 + p_2 q_1}.$$

## 5.4 Heron triangles with sides in arithmetic progression

Consider a primitive Heron triangle with sides in arithmetic progression. By Proposition 5.1, the sidelengths are  $2a - d, 2a, 2a + d$  for integers  $a$  and  $d$ . The semiperimeter being  $s = 3a$ , we require  $(3a)(a)(a + d)(a - d) = 3a^2(a^2 - d^2)$  to be an integer. This means

$$a^2 - d^2 = 3b^2 \tag{5.2}$$

for an integer  $b$ . With  $x = \frac{a}{d}, y = \frac{b}{d}$ , we transform this condition into  $x^2 - 3y^2 = 1$ . The Heron triangles with sides in arithmetic progression, therefore, correspond to the *rational* points in the first quadrant on the curve  $x^2 - 3y^2 = 1$ . Now, such rational points can be parametrized as

$$(x, y) = \left( \frac{1 + 3t^2}{1 - 3t^2}, \frac{2t}{1 - 3t^2} \right), \quad 0 < t < \frac{1}{\sqrt{3}}.$$

The integer solutions of (5.2) are therefore

$$a = p^2 + 3q^2, \quad d = p^2 - 3q^2, \quad b = 2pq$$

for relatively prime  $p, q$  satisfying  $p^2 > 3q^2$ . This gives a Heron triangle  $(2a - d, 2a, 2a + d; 3ab)$ . In each case, we obtain a primitive Heron triangle by dividing the sidelengths by the  $g = \gcd(2a, d)$  (and correspondingly  $\Delta$  by  $g^2$ ).

Here are the primitive Heron triangles with sides in A.P., generated by taking  $p \leq 7$ :<sup>1</sup>

$p$	$q$	$(a, b, c; \Delta)$
2	1	(13, 14, 15; 84)
3	1	(3, 4, 5; 6)
4	1	(25, 38, 51; 456)
5	1	(17, 28, 39; 210)
5	2	(61, 74, 87; 2220)
6	1	(15, 26, 37; 156)
7	1	(29, 52, 75; 546)
7	2	(85, 122, 159; 5124)
7	3	(65, 76, 87; 2394)
7	4	(193, 194, 195; 16296)

<sup>1</sup>Note that some of these Heron triangles have consecutive integers as sidelengths, namely (3, 4, 5; 6), (13, 14, 15; 84), and (193, 194, 195; 1629). These correspond to  $d = 1$ . We shall treat this case in detail when we study the Pell equation. There is one such “small” triangle missing from the table, corresponding to  $(p, q) = (9, 5)$ .

**Exercise**

Is there a Heron triangle whose sides are in geometric progression?

**5.5 Heron triangles with integer inradii**

We determine all Heron triangles with a given positive integer  $r$  as inradius. This is equivalent to the solution of

$$uvw = r^2(u + v + w) \quad (5.3)$$

in positive integers  $u, v, w$ . We shall assume  $u \geq v \geq w$  (so that  $A \leq B \leq C$ ). The Heron triangle in question has sides  $a = v + w$ ,  $b = w + u$ , and  $c = u + v$ . We shall distinguish between three cases. In each case, we find appropriate bounds for  $v$  and  $w$  to determine if the corresponding  $u$  is an integer.

**Proposition 5.2.** (1) *For obtuse Heron triangles with given inradius  $r$ , it is enough to check if*

$$u = \frac{r^2(v + w)}{vw - r^2}. \quad (5.4)$$

*is an integer for  $w < r$  and  $\frac{r^2}{w} < v < \frac{r(r + \sqrt{r^2 + w^2})}{w}$ .*

(2) *For acute Heron triangles with given inradius  $r$ , it is enough to check if  $u$  given by (5.4) is integer for*

$$w < \sqrt{3}r \quad \text{and} \quad w \leq v \leq (\sqrt{2} + 1)r.$$

(3) *For Pythagorean triangles with given inradius  $r$ , it is enough to check if  $u = \frac{r(v+r)}{v-r}$  is an integer for  $r < v < (\sqrt{2} + 1)r$ .*

*Proof.* The expression (5.4) follows easily from (5.3).

(1) Since  $\frac{C}{2} \geq \frac{\pi}{4}$ ,  $w < r$ . Clearly  $vw - r^2 > 0$ . From  $u = \frac{r^2(v+w)}{vw-r^2} \geq v$ , we have, after clearing denominator,  $wv^2 - 2r^2v - r^2w < 0$ . Hence,  $\frac{r^2}{w} < v < \frac{r(r + \sqrt{r^2 + w^2})}{w}$ .

(2) If the triangle is acute angled, all  $u, v, w$  are greater than  $r$ . Since  $\frac{C}{2} > \frac{\pi}{6}$ ,  $\frac{r}{w} > \tan \frac{\pi}{3} = \frac{1}{\sqrt{3}}$ , we have  $w < \sqrt{3}r$ . Also,  $\frac{B}{2} > \frac{\pi}{8}$ . This means  $\frac{r}{v} > \frac{1}{\sqrt{2}+1}$  and  $v < (\sqrt{2} + 1)r$ .

(3) In the Pythagorean case,  $r = w$ , so that (5.3) becomes  $uv = r(u + v + r)$ , and  $u = \frac{r(v+r)}{v-r} \geq v$ . By clearing denominator,  $r(v+r) \leq v(v-r)$ ,  $v^2 - 2rv - r^2 \leq 0$ ,  $(v - r)^2 \leq 2r^2$ ,  $v < (\sqrt{2} + 1)r$ .  $\square$

**Example 5.1.** A Heron triangle is said to be perfect if its area is numerically equal to its perimeter. Equivalently, a perfect Heron triangle has inradius 2. Using Proposition 5.2 above,

(i) for obtuse triangles, we need only check  $w = 1$ , and  $4 < v \leq 8$ . For  $v = 5, 6, 8$ , the corresponding  $u$  is an integer. These give three obtuse Heron triangles.

$w$	$v$	$u$	$(a, b, c; \Delta)$
1	5	24	(6, 25, 29; 60)
1	6	14	(7, 15, 20; 42)
1	8	9	(9, 10, 17; 36)

(ii) There is no acute Heron triangle with inradius 2. We need only check  $w = 3$  and  $v = 3, 4$ .

(iii) The only Pythagorean triangles with inradius 2 are (6, 8, 10; 24) and (5, 12, 13; 30).

## 5.6 Impossibility of a Heron triangle with one side twice another

Is there a Heron triangle in which one side is twice another? <sup>2</sup> Consider a rational triangle with sides  $t_1(t_2 + t_3)$ ,  $t_2(t_3 + t_1)$  and  $t_3(t_1 + t_2)$ , with  $t_1, t_2, t_3$  satisfying  $t_1t_2 + t_2t_3 + t_3t_1 = 1$ . The condition  $2 = \frac{t_1(t_2+t_3)}{t_2(t_1+t_3)}$  reduces to

$$t_1t_2^2 - 2(1 + t_1^2)t_2 + t_1 = 0.$$

This has rational solution in  $t_2$  if and only if  $(1 + t_1^2)^2 - t_1^2 = 1 + t_1^2 + t_1^4$  is the square of a rational number. Equivalently, writing  $t_1 = \frac{y}{x}$ , we have  $x^4 + x^2y^2 + y^4 = \square$ . This is impossible by Theorem 4.4.

<sup>2</sup>This is Problem 1193 of *Crux Mathematicorum*.

Appendix: Primitive Heron triangles with sides  $< 100$ 

$(a, b, c, \Delta)$	$(a, b, c, \Delta)$	$(a, b, c, \Delta)$	$(a, b, c, \Delta)$	$(a, b, c, \Delta)$
(3, 4, 5, 6)	(5, 5, 6, 12)	(5, 5, 8, 12)	(5, 12, 13, 30)	(10, 13, 13, 60)
(4, 13, 15, 24)	(13, 14, 15, 84)	(9, 10, 17, 36)	(8, 15, 17, 60)	(16, 17, 17, 120)
(11, 13, 20, 66)	(7, 15, 20, 42)	(10, 17, 21, 84)	(13, 20, 21, 126)	(13, 13, 24, 60)
(12, 17, 25, 90)	(7, 24, 25, 84)	(14, 25, 25, 168)	(3, 25, 26, 36)	(17, 25, 26, 204)
(17, 25, 28, 210)	(20, 21, 29, 210)	(6, 25, 29, 60)	(17, 17, 30, 120)	(11, 25, 30, 132)
(5, 29, 30, 72)	(8, 29, 35, 84)	(15, 34, 35, 252)	(25, 29, 36, 360)	(19, 20, 37, 114)
(15, 26, 37, 156)	(13, 30, 37, 180)	(12, 35, 37, 210)	(24, 37, 37, 420)	(16, 25, 39, 120)
(17, 28, 39, 210)	(25, 34, 39, 420)	(10, 35, 39, 168)	(29, 29, 40, 420)	(13, 37, 40, 240)
(25, 39, 40, 468)	(15, 28, 41, 126)	(9, 40, 41, 180)	(17, 40, 41, 336)	(18, 41, 41, 360)
(29, 29, 42, 420)	(15, 37, 44, 264)	(17, 39, 44, 330)	(13, 40, 45, 252)	(25, 25, 48, 168)
(29, 35, 48, 504)	(21, 41, 50, 420)	(39, 41, 50, 780)	(26, 35, 51, 420)	(20, 37, 51, 306)
(25, 38, 51, 456)	(13, 40, 51, 156)	(27, 29, 52, 270)	(25, 33, 52, 330)	(37, 39, 52, 720)
(15, 41, 52, 234)	(5, 51, 52, 126)	(25, 51, 52, 624)	(24, 35, 53, 336)	(28, 45, 53, 630)
(4, 51, 53, 90)	(51, 52, 53, 1170)	(26, 51, 55, 660)	(20, 53, 55, 528)	(25, 39, 56, 420)
(53, 53, 56, 1260)	(33, 41, 58, 660)	(41, 51, 58, 1020)	(17, 55, 60, 462)	(15, 52, 61, 336)
(11, 60, 61, 330)	(22, 61, 61, 660)	(25, 52, 63, 630)	(33, 34, 65, 264)	(20, 51, 65, 408)
(12, 55, 65, 198)	(33, 56, 65, 924)	(14, 61, 65, 420)	(36, 61, 65, 1080)	(16, 63, 65, 504)
(32, 65, 65, 1008)	(35, 53, 66, 924)	(65, 65, 66, 1848)	(21, 61, 68, 630)	(43, 61, 68, 1290)
(7, 65, 68, 210)	(29, 65, 68, 936)	(57, 65, 68, 1710)	(29, 52, 69, 690)	(37, 37, 70, 420)
(9, 65, 70, 252)	(41, 50, 73, 984)	(26, 51, 73, 420)	(35, 52, 73, 840)	(48, 55, 73, 1320)
(19, 60, 73, 456)	(50, 69, 73, 1656)	(25, 51, 74, 300)	(25, 63, 74, 756)	(35, 44, 75, 462)
(29, 52, 75, 546)	(32, 53, 75, 720)	(34, 61, 75, 1020)	(56, 61, 75, 1680)	(13, 68, 75, 390)
(52, 73, 75, 1800)	(40, 51, 77, 924)	(25, 74, 77, 924)	(68, 75, 77, 2310)	(41, 41, 80, 360)
(17, 65, 80, 288)	(9, 73, 80, 216)	(39, 55, 82, 924)	(35, 65, 82, 1092)	(33, 58, 85, 660)
(29, 60, 85, 522)	(39, 62, 85, 1116)	(41, 66, 85, 1320)	(36, 77, 85, 1386)	(13, 84, 85, 546)
(41, 84, 85, 1680)	(26, 85, 85, 1092)	(72, 85, 85, 2772)	(34, 55, 87, 396)	(52, 61, 87, 1560)
(38, 65, 87, 1140)	(44, 65, 87, 1386)	(31, 68, 87, 930)	(61, 74, 87, 2220)	(65, 76, 87, 2394)
(53, 75, 88, 1980)	(65, 87, 88, 2640)	(41, 50, 89, 420)	(28, 65, 89, 546)	(39, 80, 89, 1560)
(21, 82, 89, 840)	(57, 82, 89, 2280)	(78, 89, 89, 3120)	(53, 53, 90, 1260)	(17, 89, 90, 756)
(37, 72, 91, 1260)	(60, 73, 91, 2184)	(26, 75, 91, 840)	(22, 85, 91, 924)	(48, 85, 91, 2016)
(29, 75, 92, 966)	(39, 85, 92, 1656)	(34, 65, 93, 744)	(39, 58, 95, 456)	(41, 60, 95, 798)
(68, 87, 95, 2850)	(73, 73, 96, 2640)	(37, 91, 96, 1680)	(51, 52, 97, 840)	(65, 72, 97, 2340)
(26, 73, 97, 420)	(44, 75, 97, 1584)	(35, 78, 97, 1260)	(75, 86, 97, 3096)	(11, 90, 97, 396)
(78, 95, 97, 3420)				



## Chapter 6

# Sums of two and four squares

### 6.1 Euler's proof of Fermat's two-square theorem

**Theorem 6.1.** *Let  $p$  be an odd prime.  $p$  is a sum of two squares if and only if  $p \equiv 1 \pmod{4}$ . In this case, the expression is unique.*

*Proof.* Since  $p \equiv 1 \pmod{4}$ , the equation  $x^2 + y^2 = mp$  is solvable in integers for some  $m$ . We want to show that the *smallest* possible value of  $m$  is 1. Note that we may choose  $|x|, |y| < \frac{p}{2}$  so that  $m < \frac{p}{2}$ . If  $m \neq 1$ , it cannot divide *both* of  $x$  and  $y$ , for otherwise  $m^2 | x^2 + y^2 = mp$  and  $m | p$ , contrary to  $m < \frac{p}{2}$ . Now choose integers  $a$  and  $b$  such that  $x_1 = x - am$  and  $y_1 = y - bm$  satisfy  $|x_1|, |y_1| \leq \frac{m}{2}$ . Note that  $x_1$  and  $y_1$  cannot be both zero, and

$$0 < x_1^2 + y_1^2 \leq \frac{m^2}{2}.$$

It follows that  $x_1^2 + y_1^2 = m'm$  for some  $m' \leq \frac{m}{2} < m$ . Now,

$$m^2 m' p = (x^2 + y^2)(x_1^2 + y_1^2) = (xx_1 + yy_1)^2 + (xy_1 - yx_1)^2,$$

and

$$\begin{aligned} xx_1 + yy_1 &= x(x - am) + y(y - bm) = (x^2 + y^2) - (ax + by)m = mX \\ xy_1 - yx_1 &= x(y - bm) - y(x - am) = m(-bx + ay) = mY \end{aligned}$$

for some  $X$  and  $Y$ . From this it follows that

$$X^2 + Y^2 = m'p$$

with  $m' < m$ . By *descent*, we finally reach an equation  $x^2 + y^2 = p$ .

Uniqueness: If  $p = a^2 + b^2 = x^2 + y^2$ , where  $a < b$  and  $x < y$  are all positive, then

$$p^2 = (a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2 = (ax - by)^2 + (ay + bx)^2$$

Note that

$$(ax + by)(ay + bx) = ab(x^2 + y^2) + (a^2 + b^2)xy = p(ab + xy).$$

This means that one of  $ax + by$  and  $ay + bx$  is divisible by  $p$ . Since  $ax + by, ay + bx \leq p$ , we must have  $ay - bx = 0$  or  $ax - by = 0$ . In other words,  $\frac{x}{y} = \frac{a}{b}$  or  $\frac{b}{a}$ . Indeed,  $\frac{x}{y} = \frac{a}{b}$ . It follows that we must have  $x = a$  and  $y = b$ .  $\square$

## 6.2 Representation of integers as sums of two squares

We say that a representation  $n = x^2 + y^2$  is *primitive* if  $\gcd(x, y) = 1$ .

**Lemma 6.2.** *If  $n$  has a prime divisor  $q \equiv 3 \pmod{4}$ , then it does not have a primitive representation.*

*Proof.* Suppose to the contrary that  $n = x^2 + y^2$  is a primitive representation. Since  $q$  divides  $n$ , it does not divide any of  $x$  and  $y$ . In the field  $\mathbb{Z}_q$ , we write  $y = ax$  for some  $a$ . This means that  $0 = x^2 + y^2 = x^2(1 + a^2)$ . Since  $x \neq 0$ , we have  $a^2 = -1$  in  $\mathbb{Z}_q$ ,  $q \equiv 3 \pmod{4}$ , a contradiction.  $\square$

**Theorem 6.3.**

$$n = 2^a \prod_i p_i^{b_i} \prod_j q_j^{c_j}$$

*be the prime factorization of  $n$  in which the  $p$ 's and  $q$ 's are respectively primes of the form  $4k + 1$  and  $4k + 3$ . The number  $n$  is expressible as a sum of two squares if and only if each of the exponents  $c_j$  is even.*

*Proof.* (Sufficiency) Since  $2 = 1^2 + 1^2$ , and every  $p_i$  is a sum of two squares, if every  $c_j$  is even, by repeatedly using the composition formula

$$(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2$$

we easily obtain  $n$  as a sum of two squares.

(Necessity) Let  $n$  be divisible by a prime  $q \equiv 3 \pmod{4}$ , with *highest* power  $q^c$ ,  $c$  *odd*. Consider a representation  $n = x^2 + y^2$ , with  $\gcd(x, y) = d > 1$ . Let  $q^{c'}$  be the *highest* power of  $q$  dividing  $d$ . (Possibly,  $c' = 0$ ). Write  $x = dX$ ,  $y = dY$ . Then  $\gcd(X, Y) = 1$ . Let  $N = X^2 + Y^2$ . The highest power of  $q$  dividing  $N$  is  $q^{c-2c'}$ . This is positive since  $c$  is odd, contradicting Lemma 6.2 above.  $\square$

### 6.3 Lagrange's proof of the four-square theorem

**Theorem 6.4.** *Every positive integer can be represented as a sum of four squares of nonnegative integers.*

**Lemma 6.5 (4-square identity).**

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

where

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4, \\ z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3, \\ z_3 &= x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2, \\ z_4 &= x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1. \end{aligned}$$

Therefore it is enough to prove Lagrange's theorem for prime numbers.

**Lemma 6.6.** *Let  $p$  be a prime number. There are integers  $x$  and  $y$  such that  $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ .*

*Proof.* The set  $S := \{x^2 \in \mathbb{Z}_p : x \in \mathbb{Z}\}$  has exactly  $\frac{p+1}{2}$  elements; so does the set  $T := \{-(x^2 + 1) \in \mathbb{Z}_p : x \in \mathbb{Z}\}$ . Now,

$$|S \cap T| = |S| + |T| - |S \cup T| \geq \frac{p+1}{2} + \frac{p+1}{2} - p = 1.$$

Therefore, there are integers  $x$  and  $y$  satisfying  $x^2 \equiv -(y^2 + 1) \pmod{p}$ , i.e.,  $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ .  $\square$

#### 6.3.1 Descent

Let  $p$  be a prime number. There are integers  $x$  and  $y$  such that  $x^2 + y^2 + 1$  is divisible by  $p$ . We write this in the form  $x_1^2 + x_2^2 + x_3^2 + x_4^2 = kp$  for some integer  $k$ . Clearly, we may assume  $|x_1|, |x_2|, |x_3|, |x_4| \leq \frac{p-1}{2} < \frac{p}{2}$ . This means  $kp < 4 \cdot \left(\frac{p}{2}\right)^2 = p^2$  and  $k < p$ . If  $k \neq 1$ , we shall show that  $x_1, x_2, x_3, x_4$  can be replaced by another quadruple with a *smaller*  $k$ . Then, by descent, we shall ultimately reach  $k = 1$ .

Suppose  $k$  is even. We may assume  $x_1 \equiv x_2 \pmod{2}$  and  $x_3 \equiv x_4 \pmod{2}$ . Then

$$\begin{aligned} & \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 \\ &= \frac{x_1^2 + x_2^2 + x_3^2 + x_4^2}{2} \\ &= \frac{k}{2} \cdot p \end{aligned}$$

with a smaller multiplier for  $p$ .

Suppose  $k$  is odd. For  $i = 1, 2, 3, 4$ , choose  $y_i \equiv x_i$  with  $|y_i| < \frac{k}{2}$ . Note that  $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \pmod{k}$ . Write  $y_1^2 + y_2^2 + y_3^2 + y_4^2 = kq$  for some  $q < k$ . Note that  $q$  must be nonzero.<sup>1</sup>

Apply the four-square identity to the two quadruples  $x_i$  and  $y_i$ . The left hand side is  $(kp)(kq) = k^2pq$ . On the right hand side,  $z_2, z_3, z_4$  are clearly divisible by  $k$ ; so is  $z_1$  because  $z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{k}$ . Writing  $z_i = kw_i$  for  $i = 1, 2, 3, 4$ , we have, from the 4-square identity,  $w_1^2 + w_2^2 + w_3^2 + w_4^2 = pq$  for  $q < k$ .

## Chapter 7

# Finite continued fractions

### 7.1 Euler's function for the convergents of a continued fraction

Given two positive integers  $a > b$ , the gcd can be computed by successive divisions. More precisely, we form two sequences

$$r_0, r_1, r_2, \dots, r_k, \dots$$

and

$$q_1, q_2, \dots, q_k,$$

by the following rules

- (i)  $r_0 = a$  and  $r_1 = b$ ;
- (ii)  $q_k = \lfloor \frac{r_{k-1}}{r_k} \rfloor$ ;
- (iii)  $r_{k+1} = r_{k-1} - q_k r_k$ .

The sequence  $r_k$  eventually decreases to 0. If  $r_{n+1} = 0$ , then  $r_n$  is the gcd of  $a$  and  $b$ . We call the sequence  $(r_k)$  the *euclidean algorithm sequence* of  $a$  and  $b$ .

Like the sequence  $r_k$ , we use the **same** recurrence relations to generate two sequences  $s_k$  and  $t_k$ , **using the same**  $q_k$  but with different initial values

- (iv)  $s_0 = 1, s_1 = 0$ ;
- (v)  $t_0 = 0, t_1 = 1$ .

It is clear that  $r_k = as_k + bt_k$  for each  $k$ .

**Proposition 7.1.** (1)  $r_k = as_k + bt_k$  for every  $k$ . In particular,  $bt_k \equiv r_k \pmod{a}$ .

(2) The sequences  $(s_k)$  and  $(t_k)$  are alternating in sign. More precisely,

$$s_k = (-1)^k |s_k| \quad \text{and} \quad t_k = (-1)^{k+1} |t_k|,$$

for  $k = 0, 1, 2, \dots, n + 1$ .

(3) The sequences  $(|s_k|)$  and  $(|t_k|)$  satisfy

$$\begin{aligned} |s_{k+1}| &= |s_{k-1}| + q_k |s_k|, \\ |t_{k+1}| &= |t_{k-1}| + q_k |t_k|. \end{aligned}$$

(4) The sequence  $(|t_k|)$  is increasing. Consequently, the reversal of  $(|t_k|)$  is a euclidean algorithm sequence.

The euclidean algorithm sequence leads to the continued fraction expansion of the rational number  $\frac{a}{b}$ . Since

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\ddots + \frac{1}{q_{n-1} + \frac{1}{q_n}}}}}$$

For convenience, we shall write this continued fraction as

$$[q_1, q_2, q_n \dots, q_{n-1}, q_n].$$

The *convergents* of the continued fraction  $[q_1, q_2, \dots, q_n]$  are

$$\begin{aligned} [q_1] &= \frac{q_1}{1}, \\ [q_1, q_2] &= \frac{q_1 q_2 + 1}{q_2}, \\ [q_1, q_2, q_3] &= \frac{q_1 q_2 q_3 + q_1 + q_3}{q_2 q_3 + 1}, \\ [q_1, q_2, q_3, q_4] &= \frac{q_1 q_2 q_3 q_4 + q_1 q_2 + q_1 q_4 + q_2 q_3 + 1}{q_2 q_3 q_4 + q_2 + q_4}, \\ &\vdots \end{aligned}$$

These convergents are given by

$$[q_1, q_2, \dots, q_k] = \frac{F(q_1, q_2, \dots, q_k)}{F(q_2, \dots, q_k)},$$

where  $F$  is the Euler function obtained in the following way:  
 $F(q_1, q_2, \dots, q_k)$  is the sum  $q_1 q_2 \cdots q_k$  and all products obtained by deleting *pairs of consecutive factors*, with the stipulation that if  $k$  is even, deleting *all* consecutive pairs leads to the empty product 1.

Note that

$$\begin{aligned} F(q_1, q_2, \dots, q_k) &= F(q_k, \dots, q_2, q_1); \\ F(q_1, q_2, \dots, q_{k+1}) &= F(q_1, q_2, \dots, q_{k-1}) + q_{k+1} F(q_1, q_2, \dots, q_k). \end{aligned}$$

In the euclidean algorithm sequence,

$$r_k = F(q_{k+1}, q_{k+2}, \dots, q_n),$$

for  $k = 0, 1, 2, \dots, n$ .

## 7.2 Cornacchia' algorithm for a prime as a sum of two squares

**Theorem 7.2 (Cornacchia).** *Let  $p \equiv 1 \pmod{4}$  be a prime, and  $q$  the "smaller positive square root" of  $-1 \pmod{p}$ . If  $x$  and  $y$  are the first two remainders in the euclidean algorithm sequence of  $(p, q)$ , then  $p = x^2 + y^2$ .*

*Proof.* In the euclidean algorithm table for the pair  $(a, b) = (p, q)$  (ending in  $n$  divisions), we make the following observations.

- (1)  $n$  is even.
- (2) The sequence  $(|t_k|)$  is the reversal of  $(r_k)$ ; i.e.,  $|t_k| = r_{n+1-k}$  for every  $k \leq n$ .
- (3) The sequence  $(q_k)$  is palindromic; i.e.,  $q_{n+1-k} = q_k$  for every  $k \leq n$ .
- (4)  $r_k^2 + t_k^2$  is divisible by  $p$  for every  $k$ .
- (5) Let  $n = 2m$ . In the sequence  $(r_k)$ ,  $r_m$  is the *first* term smaller than  $\sqrt{p}$ .

Clearly,  $|t_{n+1}| = p$ . Since  $r_n = 1$ , we have  $qt_n \equiv 1 \pmod{p}$ , and  $t_n \equiv -q \pmod{p}$ . It follows that  $t_n = -q$  or  $p - q$ . The reversal of  $(|t_k|)$  is a euclidean algorithm sequence ending in exactly  $n$  divisions (as the sequence  $(r_k)$ ). If  $|t_n| = p - x$ , the sequence of division would be

$$p, p - q, q, \dots$$

which would be *longer* than the division sequence of  $(p, q)$ , a contradiction. Thus,

- (1)  $n$  is even, and  
 (2) the reversal of sequence  $(|t_k|)$  is the euclidean algorithm sequence of  $(p, q)$ , which is exactly the sequence  $(r_k)$ .  
 (3) is an immediate consequence of (2).  
 (4) follows from  $qt_k \equiv r_k \pmod{p}$ . Squaring, we have  $r_k^2 \equiv q^2 t_k^2 \equiv -t_k^2 \pmod{p}$ , and  $r_k^2 + t_k^2 \equiv 0 \pmod{p}$ .  
 (5) Write  $n = 2m$ . Note that  $r_m = F(q_{m+1}, q_{m+2}, \dots, q_{2m})$ , and  $p = r_0 = F(q_1, q_2, \dots, q_{2m})$ . Now,

$$\begin{aligned}
 r_m^2 &= r_m \cdot r_m \\
 &= F(q_{m+1}, q_{m+2}, \dots, q_{2m}) F(q_{m+1}, q_{m+2}, \dots, q_{2m}) \\
 &= F(q_m, q_{m-1}, \dots, q_1) F(q_{m+1}, q_{m+2}, \dots, q_{2m}) \\
 &= F(q_1, q_2, \dots, q_m) F(q_{m+1}, q_{m+2}, \dots, q_{2m}).
 \end{aligned}$$

It is clear that each term in the product is contained in  $F(q_1, q_2, \dots, q_{2m})$ . This shows that  $r_m^2 < p$ . On the other hand,

$$\begin{aligned}
 r_{m-1}^2 &= r_{m-1} \cdot r_{m-1} \\
 &= F(q_m, q_{m+1}, q_{m+2}, \dots, q_{2m}) F(q_m, q_{m+1}, q_{m+2}, \dots, q_{2m}) \\
 &= F(q_{m+1}, q_m, q_{m-1}, \dots, q_1) F(q_m, q_{m+1}, q_{m+2}, \dots, q_{2m}) \\
 &= F(q_1, q_2, \dots, q_m, q_{m+1}) F(q_m, q_{m+1}, q_{m+2}, \dots, q_{2m}).
 \end{aligned}$$

Every product in  $F(q_1, q_2, \dots, q_{2m})$  is contained in this product. This shows that  $r_{m-1}^2 > p$ .

Now, since  $r_m^2 + r_{m+1}^2 = r_m^2 + t_{n-m}^2 = r_m^2 + t_m^2$  is divisible by  $p$ , and  $r_{m+1} < r_m < \sqrt{p}$ , the sum  $r_m^2 + r_{m+1}^2$  being positive and smaller than  $2p$ , must be  $p$ .  $\square$

## Chapter 8

# Quadratic Residues

Let  $n > 1$  be a given positive integer, and  $\gcd(a, n) = 1$ . We say that  $a \in \mathbb{Z}_n^\bullet$  is a *quadratic residue mod  $n$*  if the congruence  $x^2 \equiv a \pmod{n}$  is solvable. Otherwise,  $a$  is called a *quadratic nonresidue mod  $n$* .

1. If  $a$  and  $b$  are quadratic residues mod  $n$ , so is their product  $ab$ .
2. If  $a$  is a quadratic residue, and  $b$  a quadratic nonresidue mod  $n$ , then  $ab$  is a quadratic nonresidue mod  $n$ .
3. The product of two quadratic residues mod  $n$  is not necessarily a quadratic residue mod  $n$ . For example, in  $\mathbb{Z}_{12}^\bullet = \{1, 5, 7, 11\}$ , only 1 is a quadratic residue; 5, 7, and  $11 \equiv 5 \cdot 7$  are all quadratic nonresidues.

**Theorem 8.1.** *Let  $p$  be an odd prime. Exactly one half of the elements of  $\mathbb{Z}_p^\bullet$  are quadratic residues.*

*Proof.* Each quadratic residue modulo  $p$  is congruent to one of the following  $\frac{1}{2}(p-1)$  residues.

$$1^2, 2^2, \dots, k^2, \dots, \left(\frac{p-1}{2}\right)^2.$$

We show that these residue classes are all distinct. For  $1 \leq h < k \leq \frac{p-1}{2}$ ,  $h^2 \equiv k^2 \pmod{p}$  if and only if  $(k-h)(h+k)$  is divisible by  $p$ , this is impossible since each of  $k-h$  and  $h+k$  is smaller than  $p$ .  $\square$

**Corollary 8.2.** *If  $p$  is an odd prime, the product of two quadratic nonresidues is a quadratic residue.*

**Theorem 8.3.** *Let  $p$  be an odd prime.  $-1$  is a quadratic residue mod  $p$  if and only if  $p \equiv 1 \pmod{4}$ .*

*Proof.* If  $x^2 \equiv -1 \pmod{p}$ , then  $(-1)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$  by Fermat's little theorem. This means that  $\frac{p-1}{2}$  is even, and  $p \equiv 1 \pmod{4}$ .

Conversely, if  $p \equiv 1 \pmod{4}$ , the integer  $\frac{p-1}{2}$  is even. By Wilson's theorem,

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 = \prod_{i=1}^{\frac{p-1}{2}} j^2 = \prod_{i=1}^{\frac{p-1}{2}} j \cdot (-j) \equiv \prod_{i=1}^{\frac{p-1}{2}} j \cdot (p-j) = (p-1)! \equiv -1 \pmod{p}.$$

The solutions of  $x^2 \equiv -1 \pmod{p}$  are therefore  $x \equiv \pm \left(\frac{p-1}{2}\right)!$ .  $\square$

Here are the square roots of  $-1 \pmod{p}$  for the first 20 primes of the form  $4k + 1$ :

$p$	$\sqrt{-1}$	$p$	$\sqrt{-1}$	$p$	$\sqrt{-1}$	$p$	$\sqrt{-1}$	$p$	$\sqrt{-1}$
5	$\pm 2$	13	$\pm 5$	17	$\pm 4$	29	$\pm 12$	37	$\pm 6$
41	$\pm 9$	53	$\pm 23$	61	$\pm 11$	73	$\pm 27$	89	$\pm 34$
97	$\pm 22$	101	$\pm 10$	109	$\pm 33$	113	$\pm 15$	137	$\pm 37$
149	$\pm 44$	157	$\pm 28$	173	$\pm 80$	181	$\pm 19$	193	$\pm 81$

**Theorem 8.4.** *There are infinitely many primes of the form  $4n + 1$ .*

*Proof.* Suppose there are only finitely many primes  $p_1, p_2, \dots, p_r$  of the form  $4n + 1$ . Consider the product

$$P = (2p_1 p_2 \cdots p_r)^2 + 1.$$

Note that  $P \equiv 1 \pmod{4}$ . Since  $P$  is greater than each of  $p_1, p_2, \dots, p_r$ , it cannot be prime, and so must have a prime factor  $p$  different from  $p_1, p_2, \dots, p_r$ . But then modulo  $p$ ,  $-1$  is a square. By Theorem 8.3,  $p$  must be of the form  $4n + 1$ , a contradiction.  $\square$

In the table below we list, for primes  $< 40$ , the quadratic residues and their square roots. It is understood that the square roots come in pairs. For example, the entry (2,7) for the prime 47 should be interpreted as saying that the *two* solutions of the congruence  $x^2 \equiv 2 \pmod{47}$  are  $x \equiv \pm 7 \pmod{47}$ . Also, for primes of the form  $p = 4n + 1$ , since  $-1$  is a quadratic residue modulo  $p$ , we only list quadratic residues smaller than  $\frac{p}{2}$ . Those greater than  $\frac{p}{2}$  can be found with the help of the square roots of  $-1$ .

3		(1,1)							
5	(-1,2)	(1,1)							
7		(1,1)	(2,3)	(4,2)					
11		(1,1)	(3,5)	(4,2)	(5,4)	(9,3)			
13	(-1,5)	(1,1)	(3,4)	(4,2)					
17	(-1,4)	(1,1)	(2,6)	(4,2)	(8,5)				
19		(1,1)	(4,2)	(5,9)	(6,5)	(7,8)	(9,3)	(11,7)	(16,4)
		(17,6)							
23		(1,1)	(2,5)	(3,7)	(4,2)	(6,11)	(8,10)	(9,3)	(12,9)
		(13,6)	(16,4)	(18,8)					
29	(-1,12)	(1,1)	(4,2)	(5,11)	(6,8)	(7,6)	(9,3)	(13,10)	
31		(1,1)	(2,8)	(4,2)	(5,6)	(7,10)	(8,15)	(9,3)	(10,14)
		(14,13)	(16,4)	(18,7)	(19,9)	(20,12)	(25,5)	(28,11)	
37	(-1,6)	(1,1)	(3,15)	(4,2)	(7,9)	(9,3)	(10,11)	(11,14)	(12,7)
		(16,4)							

## 8.1 The Legendre symbol

Let  $p$  be an *odd* prime. For an integer  $a$ , we define the **Legendre symbol**

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{if } a \text{ is a quadratic residue mod } p, \\ -1, & \text{otherwise.} \end{cases}$$

**Lemma 8.5.**  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$ .

*Proof.* This is equivalent to saying that modulo  $p$ , the product of two quadratic residues (respectively nonresidues) is a quadratic residue, and the product of a quadratic residue and a quadratic nonresidue is a quadratic nonresidue.  $\square$

For an odd prime  $p$ ,  $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$ . This is a restatement of Theorem 8.3 that  $-1$  is a quadratic residue mod  $p$  if and only if  $p \equiv 1 \pmod{4}$ .

**Theorem 8.6 (Euler).** *Let  $p$  be an odd prime. For each integer  $a$  not divisible by  $p$ ,*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \pmod{p}.$$

*Proof.* Suppose  $a$  is a quadratic *nonresidue* mod  $p$ . The mod  $p$  residues  $1, 2, \dots, p-1$  are partitioned into pairs satisfying  $xy = a$ . In this case,

$$(p-1)! \equiv a^{\frac{1}{2}(p-1)} \pmod{p}.$$

On the other hand, if  $a$  is a quadratic *residue*, with  $a \equiv k^2 \equiv (p - k)^2 \pmod{p}$ , apart from  $0, \pm k$ , the remaining  $p - 3$  elements of  $\mathbb{Z}_p$  can be partitioned into pairs satisfying  $xy = a$ .

$$(p - 1)! \equiv k(p - k)a^{\frac{1}{2}(p-3)} \equiv -a^{\frac{1}{2}(p-1)} \pmod{p}.$$

Summarizing, we obtain

$$(p - 1)! \equiv - \left( \frac{a}{p} \right) a^{\frac{1}{2}(p-1)} \pmod{p}.$$

Note that by putting  $a = 1$ , we obtain *Wilson's theorem*:  $(p - 1)! \equiv -1 \pmod{p}$ . By comparison, we obtain a formula for  $\left( \frac{a}{p} \right)$ :

$$\left( \frac{a}{p} \right) \equiv a^{\frac{1}{2}(p-1)} \pmod{p}.$$

□

**Theorem 8.7 (Gauss' Lemma).** *Let  $p$  be an odd prime, and  $a$  an integer not divisible by  $p$ . Then  $\left( \frac{a}{p} \right) = (-1)^\mu$  where  $\mu$  is the number of residues among*

$$a, 2a, 3a, \dots, \frac{p-1}{2}a$$

*falling in the range  $\frac{p}{2} < x < p$ .*

*Proof.* Every residue modulo  $p$  has a unique representative with least absolute value, namely, the one in the range  $-\frac{p-1}{2} \leq x \leq \frac{p-1}{2}$ . The residues described in the statement of Gauss' Lemma are precisely those whose representatives are *negative*. Now, among the representatives of the residues of

$$a, 2a, \dots, \frac{p-1}{2}a,$$

say, there are  $\lambda$  **positive** ones,

$$r_1, r_2, \dots, r_\lambda,$$

and  $\mu$  **negative** ones

$$-s_1, -s_2, \dots, -s_\mu.$$

Here,  $\lambda + \mu = \frac{p-1}{2}$ , and  $0 < r_i, s_j < \frac{p}{2}$ .

Note that no two of the  $r$ 's are equal; similarly for the  $s$ 's. Suppose that  $r_i = s_j$  for some indices  $i$  and  $j$ . This means

$$ha \equiv r_i \pmod{p}; \quad ka \equiv -s_j \pmod{p}$$

for some  $h, k$  in the range  $0 < h, k < \frac{1}{2}(p-1)$ . Note that  $(h+k)a \equiv 0 \pmod{p}$ . But this is a contradiction since  $h+k < p-1$  and  $p$  does not divide  $a$ . It follows that

$$r_1, r_2, \dots, r_\lambda, s_1, s_2, \dots, s_\mu$$

are a permutation of  $1, 2, \dots, \frac{1}{2}(p-1)$ . From this

$$a \cdot 2a \cdots \frac{p-1}{2}a = (-1)^\mu 1 \cdot 2 \cdots \frac{p-1}{2},$$

and  $a^{\frac{1}{2}(p-1)} = (-1)^\mu$ . By Theorem 8.6,  $\left(\frac{a}{p}\right) = (-1)^\mu$ .  $\square$

### Example

Let  $p = 19$  and  $a = 5$ . We consider the first 9 multiples of 5 mod 19. These are

$$5, 10, 15, 20 \equiv 1, 25 \equiv 6, 30 \equiv 11, 35 \equiv 16, 40 \equiv 2, 45 \equiv 7.$$

4 of these exceed 9, namely, 10, 15, 11, 16. It follows that  $\left(\frac{5}{19}\right) = 1$ ; 5 is a quadratic residue mod 19.<sup>1</sup>

### Theorem 8.8.

$$\left(\frac{2}{p}\right) = (-1)^{\lfloor \frac{1}{4}(p+1) \rfloor} = (-1)^{\frac{1}{8}(p^2-1)}.$$

Equivalently,  $\left(\frac{2}{p}\right) = +1$  if and only if  $p \equiv \pm 1 \pmod{8}$ .

*Proof.* We need to see how many terms in the sequence

$$2 \cdot 1, \quad 2 \cdot 2, \quad 2 \cdot 3, \quad \dots, \quad 2 \cdot \frac{p-1}{2}$$

are in the range  $\frac{p}{2} < x < p$ . If  $p = 4k + 1$ , these are the numbers  $2k + 2, \dots, 4k$ , and there are  $k$  of them. On the other hand, if  $p = 4k + 3$ , these are the numbers  $2k + 2, \dots, 4k + 2$ , and there are  $k + 1$  of them. In each case, the number of terms is  $\lfloor \frac{1}{4}(p+1) \rfloor$ .  $\square$

<sup>1</sup>Indeed  $5 \equiv 9^2 \pmod{19}$ .

**Example**

Square root of 2 mod  $p$  for the first 20 primes of the form  $8k \pm 1$ .

$p$	$\sqrt{2}$	$p$	$\sqrt{2}$	$p$	$\sqrt{2}$	$p$	$\sqrt{2}$	$p$	$\sqrt{2}$
7	3	17	6	23	5	31	8	41	17
47	7	71	12	73	32	79	9	89	25
97	14	103	38	113	51	127	16	137	31
151	46	167	13	191	57	193	52	199	20

**8.2 The law of quadratic reciprocity**

**Theorem 8.9 (Law of quadratic reciprocity).** *Let  $p$  and  $q$  be distinct odd primes.*

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

*Equivalently, when at least one of  $p, q \equiv 1 \pmod{4}$ ,  $p$  is a quadratic residue mod  $q$  if and only if  $q$  is a quadratic residue mod  $p$ .<sup>2</sup>*

*Proof.* (1) Let  $a$  be an integer not divisible by  $p$ . Suppose, as in the proof of Gauss' Lemma above, of the residues  $a, 2a, \dots, \frac{p-1}{2}a$ , the *positive* least absolute value representatives are  $r_1, r_2, \dots, r_\lambda$ , and the *negative* ones are  $-s_1, -s_2, \dots, -s_\mu$ . The numbers  $a, 2a, \dots, \frac{p-1}{2}a$  are a permutation of

$$\left\lfloor \frac{h_i a}{p} \right\rfloor p + r_i, \quad i = 1, 2, \dots, \lambda,$$

and

$$\left\lfloor \frac{k_j a}{p} \right\rfloor p + (p - s_j), \quad j = 1, 2, \dots, \mu,$$

where  $h_1, \dots, h_\lambda, k_1, \dots, k_\mu$  are a permutation of  $1, 2, \dots, \frac{p-1}{2}$ . Con-

---

<sup>2</sup>For  $p \equiv q \equiv 3 \pmod{4}$ ,  $p$  is a quadratic residue mod  $q$  if and only if  $q$  is a quadratic nonresidue mod  $p$ .

sidering the sum of these numbers, we have

$$\begin{aligned}
 a \cdot \sum_{m=1}^{\frac{1}{2}(p-1)} m &= p \sum_{m=1}^{\frac{1}{2}(p-1)} \left[ \frac{ma}{p} \right] + \sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{\mu} (p - s_j) \\
 &= p \sum_{m=1}^{\frac{1}{2}(p-1)} \left[ \frac{ma}{p} \right] + \sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{\mu} s_j + \sum_{j=1}^{\mu} (p - 2s_j) \\
 &= p \sum_{m=1}^{\frac{1}{2}(p-1)} \left[ \frac{ma}{p} \right] + \sum_{m=1}^{\frac{1}{2}(p-1)} m + \mu \cdot p - 2 \sum_{j=1}^{\mu} s_j.
 \end{aligned}$$

In particular, **if  $a$  is odd**, then

$$\mu \equiv \sum_{m=1}^{\frac{1}{2}(p-1)} \left[ \frac{ma}{p} \right] \pmod{2},$$

and by Gauss' lemma,

$$\left( \frac{a}{p} \right) = (-1)^{\sum_{m=1}^{\frac{1}{2}(p-1)} \left[ \frac{ma}{p} \right]}.$$

(2) Therefore, for distinct odd primes  $p$  and  $q$ , we have

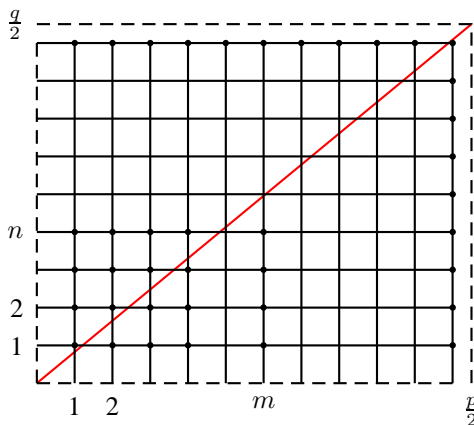
$$\left( \frac{q}{p} \right) = (-1)^{\sum_{m=1}^{\frac{1}{2}(p-1)} \left[ \frac{mq}{p} \right]},$$

and

$$\left( \frac{p}{q} \right) = (-1)^{\sum_{n=1}^{\frac{1}{2}(q-1)} \left[ \frac{np}{q} \right]}.$$

(3) In the diagram above, we consider the lattice points  $(m, n)$  with  $1 \leq m \leq \frac{p-1}{2}$  and  $1 \leq n \leq \frac{q-1}{2}$ . There are altogether  $\frac{p-1}{2} \cdot \frac{q-1}{2}$  such points forming a rectangle. These points are separated by the line  $\mathcal{L}$  of slope  $\frac{q}{p}$  through the point  $(0,0)$ .

For each  $m = 1, 2, \dots, \frac{p-1}{2}$ , the number of points in the vertical line through  $(m, 0)$  **under**  $\mathcal{L}$  is  $\left[ \frac{mq}{p} \right]$ . Therefore, the total number of points **under**  $\mathcal{L}$  is  $\sum_{m=1}^{\frac{1}{2}(p-1)} \left[ \frac{mq}{p} \right]$ . Similarly, the total number of points on the **left** side of  $\mathcal{L}$  is  $\sum_{n=1}^{\frac{1}{2}(q-1)} \left[ \frac{np}{q} \right]$ . From these, we have



$$\sum_{m=1}^{\frac{1}{2}(p-1)} \left[ \frac{mq}{p} \right] + \sum_{n=1}^{\frac{1}{2}(q-1)} \left[ \frac{np}{q} \right] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

It follows that

$$\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

□

The law of quadratic reciprocity can be recast into the following form:

$$\left( \frac{p}{q} \right) = \begin{cases} - \left( \frac{q}{p} \right), & \text{if } p \equiv q \equiv 3 \pmod{4}, \\ + \left( \frac{q}{p} \right), & \text{otherwise.} \end{cases}$$

### Examples

$$1. \left( \frac{59}{131} \right) = - \left( \frac{131}{59} \right) = - \left( \frac{13}{59} \right) = - \left( \frac{59}{13} \right) = - \left( \frac{7}{13} \right) = - \left( \frac{13}{7} \right) = - \left( \frac{-1}{7} \right) = -(-1) = 1.$$

$$2. \left( \frac{34}{97} \right) = \left( \frac{2}{97} \right) \left( \frac{17}{97} \right). \text{ Now, } \left( \frac{2}{97} \right) = +1 \text{ by Theorem 8.8, and}$$

$$\left( \frac{17}{97} \right) = \left( \frac{97}{17} \right) = \left( \frac{12}{17} \right) = \left( \frac{3}{17} \right) \left( \frac{4}{17} \right) = \left( \frac{3}{17} \right) = \left( \frac{17}{3} \right) = \left( \frac{2}{3} \right) = -1.$$

3. For which primes  $p$  is 3 a quadratic residue ?

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = (-1)^{k+\frac{1}{2}(\epsilon-1)} \epsilon = (-1)^k$$

provided  $p = 6k + \epsilon$ ,  $\epsilon = \pm 1$ . This means 3 is a quadratic residue mod  $p$  if and only if  $k$  is even, i.e.,  $p = 12m \pm 1$ .

### 8.3 Calculation of square roots modulo $p$

1. Let  $p$  be a prime of the form  $4k + 3$ . If  $\left(\frac{a}{p}\right) = 1$ , then the square roots of  $a \pmod{p}$  are  $\pm a^{\frac{1}{4}(p+1)}$ .

*Proof.*

$$\left(a^{\frac{1}{4}(p+1)}\right)^2 \equiv a^{\frac{1}{2}(p+1)} = a^{\frac{1}{2}(p-1)} \cdot a = \left(\frac{a}{p}\right) a = a \pmod{p}.$$

□

2. Let  $p$  be a prime of the form  $8k + 5$ . If  $\left(\frac{a}{p}\right) = 1$ , then the square roots of  $a \pmod{p}$  are

- $\pm a^{\frac{1}{8}(p+3)}$  if  $a^{\frac{1}{4}(p-1)} \equiv 1 \pmod{p}$ ,
- $\pm 2^{\frac{1}{4}(p-1)} \cdot a^{\frac{1}{8}(p+3)}$  if  $a^{\frac{1}{4}(p-1)} \equiv -1 \pmod{p}$ .

*Proof.* Note that

$$\left(a^{\frac{1}{8}(p+3)}\right)^2 \equiv a^{\frac{1}{4}(p+3)} = a^{\frac{1}{4}(p-1)} \cdot a \pmod{p}.$$

Since  $\left(\frac{a}{p}\right) = a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$ , we have  $a^{\frac{1}{4}(p-1)} \equiv \pm 1 \pmod{p}$ .

If  $a^{\frac{1}{4}(p-1)} \equiv 1 \pmod{p}$ , then this gives  $a^{\frac{1}{8}(p+3)}$  as a square root of  $a \pmod{p}$ .

If  $a^{\frac{1}{4}(p-1)} \equiv -1 \pmod{p}$ , then we have

$$a \equiv -\left(a^{\frac{1}{8}(p+3)}\right)^2 \equiv \left(\frac{y}{p}\right) \left(a^{\frac{1}{8}(p+3)}\right)^2 \equiv \left(y^{\frac{1}{4}(p-1)} a^{\frac{1}{8}(p+3)}\right)^2$$

for any quadratic nonresidue  $y \pmod{p}$ . Since  $p \equiv 5 \pmod{8}$ , we may simply take  $y = 2$ . □

**Examples**

1. Let  $p = 23$ . Clearly 2 is a quadratic residue mod 23. The square roots of 2 are  $\pm 2^6 \equiv \pm 18 \equiv \mp 5 \pmod{23}$ .

2. Let  $p = 29$ . Both 6 and 7 are quadratic residues mod 29.

Since  $7^7 \equiv 1 \pmod{29}$ , the square root of 7 are  $\pm 7^4 \equiv \pm 23 \mp 6 \pmod{29}$ .

On the other hand, Since  $6^7 \equiv -1 \pmod{29}$ , the square roots of 6 are  $\pm 2^7 \cdot 6^4 \equiv \pm 12 \cdot 20 \equiv \pm 8 \pmod{29}$ .

**Proposition 8.10.** *Let  $p$  be an odd prime and  $p - 1 = 2^\lambda u$ ,  $u$  odd. Consider the congruence  $x^2 \equiv a \pmod{p}$ . Let  $b$  be any quadratic non-residue mod  $p$ . Assume that  $a^u \not\equiv \pm 1 \pmod{p}$ , and that  $\mu > 1$  is the smallest integer for which  $(a^u)^{2^\mu} \equiv -1 \pmod{p}$ . If  $\mu = \lambda - 1$ , then the congruence has no solution. If  $\mu \leq \lambda - 2$ , then  $a^u \equiv (b^u)^{2^{\lambda-\mu-1}k}$  for some odd number  $k < 2^{\mu+1}$ . The solutions of the congruence are*

$$x \equiv \pm a^{\frac{1}{2}(u+1)} b^{2^{\lambda-\mu-2}(2^{\mu+1}-k)u} \pmod{p}.$$

**Example 8.1.** Consider the congruence  $x^2 \equiv 215 \pmod{257}$ . Here  $257 - 1 = 2^8 \cdot 1$ . In the notation of the above theorem,  $u = 1$ . With  $a = 215$ , the order of  $a^u = 215$  modulo 257 is 128:

$$\begin{aligned} 215^2 &\equiv 222; & 215^4 &\equiv 197; & 215^8 &\equiv 2; \\ 215^{16} &\equiv 4; & 215^{32} &\equiv 16; & 215^{64} &\equiv 256 \equiv -1. \end{aligned}$$

This means  $\mu = 6$ . Let  $b = 3$ , a quadratic nonresidue of 257. The successive powers of  $b^u \equiv 3$  are, modulo 257,

$$\begin{aligned} 3^2 &\equiv 9; & 3^4 &\equiv 81; & 3^8 &\equiv 136; \\ 3^{16} &\equiv 249; & 3^{32} &\equiv 64; & 3^{64} &\equiv 241; \\ 3^{128} &\equiv 256 \equiv -1. \end{aligned}$$

Now,  $a^u = 215$  should be an odd power of  $(b^u)^{2^{\lambda-\mu-1}} \equiv 3^2 \equiv 9$ . In fact,

$$9^3 \equiv 729 \equiv 215 \pmod{257}.$$

This means  $k = 3$ . The solutions of the congruence are

$$x \equiv \pm 215 \cdot 3^{2^0(2^7-3)} \equiv \pm 215 \cdot 3^{125} \equiv \dots \equiv \pm 230 \equiv 27 \pmod{257}.$$

## 8.4 Square roots modulo an odd prime power

The quadratic congruence  $x^2 \equiv 2 \pmod{7}$  clearly has solutions  $x \equiv \pm 3 \pmod{7}$ . We want to solve the congruence  $x^2 \equiv 2 \pmod{7^2}$  by seeking a solution of the form  $x \equiv 3 + 7b$ .

$$2 \equiv (3 + 7b)^2 = 9 + (6b) \cdot 7 + b^2 \cdot 7^2 = 2 + (1 + 6b) \cdot 7 \pmod{7^2}$$

Choose  $b$  so that  $1 + 6b \equiv 0 \pmod{7}$ . This gives  $b \equiv 1 \pmod{7}$  and  $x \equiv 10 \pmod{7^2}$ .

### Exercise

1. Show that 9, 16, 23, 30, 37, 44 are all squares modulo 49. (Of course, it is clear for 9 and 16).

*Answer:* Squares roots modulo 49:

$$\begin{array}{cccccccc} 2 & 9 & 16 & 23 & 30 & 37 & 44 \\ 10 & 3 & 45 & 38 & 31 & 24 & 17 \end{array}$$

(Note that these square roots form an arithmetic progression of common difference  $42 \pmod{49}$ ).

2. Proceed to solve the congruences  $x^2 \equiv 2 \pmod{7^3}$ , and  $x^2 \equiv 2 \pmod{7^4}$ .

**Proposition 8.11.** *Let  $p$  be an odd prime. Suppose  $x^2 \equiv a \pmod{p^k}$  has solution  $x \equiv c_k \pmod{p^k}$ . Let  $\gamma$  be the multiplicative inverse of  $2c_1 \in \mathbb{Z}_p^\bullet$ . Then with  $b_k \equiv \gamma \cdot \frac{a - c_k^2}{p^k} \pmod{p}$ , We have a solution  $c_{k+1} \equiv c_k + b_k p^k \pmod{p^{k+1}}$  of  $x^2 \equiv a \pmod{p^{k+1}}$ .*

**Example 8.2.** The solutions of the congruences  $x^2 \equiv 12345 \pmod{7^k}$  for  $k \leq 8$  are as follows:

$$\begin{array}{cccccccc} k & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ x \pmod{7^k} & 2 & 37 & 37 & 380 & 5182 & 89217 & 677462 & 3148091 \end{array}$$

The base 7 expansions of these solutions are  $x \equiv \pm 1235521052_7$ .

## 8.5 Square modulo $2^k$

Here are the squares modulo  $2^k$ , up to  $k = 7$ .

$$\begin{aligned}\mathbb{Z}_4 & : 0, 1, \\ \mathbb{Z}_8 & : 4, \\ \mathbb{Z}_{16} & : 9, \\ \mathbb{Z}_{32} & : 16, 17, 25, \\ \mathbb{Z}_{64} & : 33, 36, 41, 49, 57, \\ \mathbb{Z}_{128} & : 64, 65, 68, 73, 81, 89, 97, 100, 105, 113, 121.\end{aligned}$$

It is easy to see that the analogue of Proposition 8.2.2 is no longer true. For example, 1 is clearly a square of  $\mathbb{Z}_4$ ; but  $5 = 1 + 4$  is not a square in  $\mathbb{Z}_8$ .

Suppose  $c \in \mathbb{Z}_{2^k}$  is a square. Let  $h$  be the *smallest* integer such that  $c = (a+2^h)^2$  for some  $a \in \mathbb{Z}_{2^{h-1}}$ . Since  $c = (a+2^h)^2 = a^2 + 2^{h+1}a + 2^{2h}$ , we must have  $h + 1 < k$ , and  $h \leq k - 2$ .

From this, we infer that 5 is not a square, and the squares in  $\mathbb{Z}_8$  are 0, 1, 4. Also, apart from these, the squares in  $\mathbb{Z}_{16}$  are  $4^2 = 0$ ,  $5^2 = 9$ ,  $6^2 = 4$ , and  $7^2 = 1$ . This means that the squares in  $\mathbb{Z}_{16}$  are 0, 1, 4 and 9.

**Proposition 8.12.** *Let  $k \geq 3$ . For every square  $c \in \mathbb{Z}_{2^k}^\bullet$ ,  $c + 2^k$  is a square in  $\mathbb{Z}_{2^{k+1}}^\bullet$ .*

*Proof.* Clearly, if  $c = 1$ ,  $c + 2^k = 1 + 2^k = (1 + 2^{k-1})^2 \in \mathbb{Z}_{2^{k+1}}$ . If  $c \neq 1$ , we write  $c = (a + 2^h)^2$  for  $1 \leq h \leq k - 2$  and  $a \in \mathbb{Z}_{2^{k-3}}$ . Then,  $(a + 2^h + 2^{k-1})^2 = c + 2^k(a + 2^h) + 2^{2k-2}$ . Since  $a$  is a unit, modulo  $2^{k+1}$ , this is  $c + 2^k$ .  $\square$

**Corollary 8.13.** *A residue given in binary expansion*

$$a = (a_{k-1}a_{k-2} \cdots a_1a_0)_2,$$

*is a quadratic residue mod  $2^k$  if and only if on the right of the rightmost digit 1 there is an even number (possibly none) of zeros, and on its left there are at least two zeros.*

## Chapter 9

# The ring of Gaussian integers

### 9.1 The ring $\mathbb{Z}[i]$

#### 9.1.1 Norm and units

By the ring of Gaussian integers we mean

$$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}.$$

Each element of  $\mathbb{Z}[i]$  is called a Gaussian integer. For  $\alpha = a + bi$ , we define the **norm**  $N(\alpha) := a^2 + b^2 \in \mathbb{Z}$ . One important property of the norm is its multiplicativity:

**Lemma 9.1.** For  $\alpha, \beta \in \mathbb{Z}[i]$ ,

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

A Gaussian integer  $\alpha$  is a **unit** if it is invertible in  $\mathbb{Z}$ . If  $\alpha$  is a unit with multiplicative inverse  $\beta$ , then  $\alpha\beta = 1$  and  $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$ . This means that  $N(\alpha) = 1$  and  $\alpha = \pm 1$ , or  $\pm i$ .

**Proposition 9.2.** The only units in  $\mathbb{Z}[i]$  are  $\pm 1$  and  $\pm i$ .

#### 9.1.2 Gaussian primes

Two Gaussian integers  $\alpha$  and  $\beta$  are **associate** if  $\alpha = \varepsilon\beta$  for some unit  $\varepsilon \in \mathbb{Z}[i]$ .

#### Exercise

1. Show that the relation of being associate is an equivalence relation on  $\mathbb{Z}[i]$ .

2. Show that 2 is not a prime in  $\mathbb{Z}[i]$ .

A Gaussian integer  $\pi \in \mathbb{Z}[i]$  is **prime** if

- (i)  $\pi$  is not a unit in  $\mathbb{Z}[i]$ , and
- (ii)  $\pi = \alpha\beta \in \mathbb{Z}[i] \Rightarrow \alpha$  or  $\beta$  is a unit in  $\mathbb{Z}[i]$ .

**Proposition 9.3.** *The ring of Gaussian integers satisfies the euclidean algorithm: for  $\alpha, \beta \in \mathbb{Z}[i]$  with  $\beta \neq 0$ , there are  $\gamma$  and  $\delta \in \mathbb{Z}[i]$  satisfying*

- (i)  $\alpha = \beta\gamma + \delta$ ,
- (ii)  $N(\delta) < N(\beta)$ .

*Proof.* Regarding  $\alpha$  and  $\beta$  as complex numbers, we have  $\frac{\alpha}{\beta} = x + iy$  for **rational** numbers  $x$  and  $y$ . Let  $a$  and  $b$  be integers such that  $|x - a| \leq \frac{1}{2}$  and  $|y - b| \leq \frac{1}{2}$ . The numbers  $\gamma := a + bi$  and  $\delta := \beta((x - a) + (y - b)i)$  satisfy  $\delta = \alpha - \beta\gamma$  and so is a Gaussian integer. Since

$$\left| \frac{\delta}{\beta} \right|^2 = (x - a)^2 + (y - b)^2 \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2},$$

we have  $N(\delta) < N(\beta)$ . □

Therefore, we have a notion of gcd in  $\mathbb{Z}[i]$ . The gcd of two Gaussian integers is defined up to a unit.

**Corollary 9.4.** *The ring of Gaussian integers is a Bézout domain: for  $\alpha, \beta \in \mathbb{Z}[i]$ , there are  $\gamma, \delta \in \mathbb{Z}[i]$  such that*

$$\gcd(\alpha, \beta) = \alpha\gamma + \beta\delta.$$

**Proposition 9.5.** *The following two statements are equivalent.*

- (i)  $\pi \in \mathbb{Z}[i]$  is a prime.
- (ii)  $\pi | \alpha\beta \in \mathbb{Z}[i] \Rightarrow \pi | \alpha$  or  $\pi | \beta$ .

**Theorem 9.6.** *The primes in  $\mathbb{Z}[i]$  are precisely*

- (i) the primes  $p \equiv 3 \pmod{4}$  in  $\mathbb{Z}$ ,
- (ii)  $\pm 1 \pm i$  which have norm 2, and
- (iii)  $a + bi$  for which  $a^2 + b^2$  is an odd prime  $p \equiv 1 \pmod{4}$  in  $\mathbb{Z}$ .

**Corollary 9.7 (Unique factorization).** *Every nonzero Gaussian integer can be decomposed “uniquely” into a product of Gaussian primes: if*

$$\alpha = \pi_1 \cdots \pi_h = \psi_1 \cdots \psi_k$$

for Gaussian primes  $\pi_1, \dots, \pi_h$  and  $\psi_1, \dots, \psi_k$ , then

- (i)  $h = k$ ,
- (ii) after a suitable permutation of  $\psi_1, \dots, \psi_k$ , for  $i = 1, 2, \dots, k$ , the Gaussian primes  $\pi_i$  and  $\psi_i$  are associate.

## 9.2 An alternative proof of Fermat's two-square theorem

Since  $p \equiv 1 \pmod{4}$ ,  $-1$  is a quadratic residue. This means that there exists an integer  $a \leq \frac{p-1}{2}$  such that  $a^2 + 1$  is divisible by  $p$ . Note that  $a^2 + 1 < p^2$ .

Regarded as Gaussian integers,  $a^2 + 1 = (a+i)(a-i)$ . We claim that  $p$  does not divide  $a+i$  nor  $a-i$ ; otherwise,  $p^2 = N(p) \leq N(a+i) = a^2 + 1 < p^2$ , a contradiction. This means that  $p$  is not a prime in  $\mathbb{Z}[i]$  and there is a factorization of  $p = \alpha\beta \in \mathbb{Z}[i]$ , in which none of  $\alpha, \beta$  is a unit, *i.e.*,  $N(\alpha), N(\beta) > 1$ . It follows from

$$p^2 = N(p) = N(\alpha)N(\beta)$$

that  $N(\alpha) = N(\beta) = p$ , and  $p$  is a sum of two squares of integers.



## Chapter 10

# Construction of indecomposable Heron triangles

### 10.1 Primitive Heron triangles

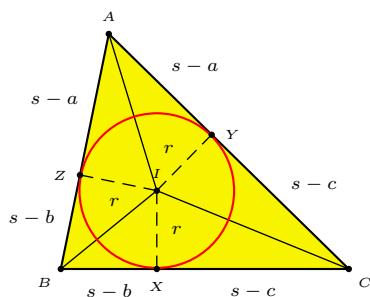
#### 10.1.1 Rational triangles

Given a triangle  $ABC$  with sidelengths  $BC = a$ ,  $CA = b$  and  $AB = c$ , we let  $s := \frac{1}{2}(a + b + c)$  be the semiperimeter, and

$$t_1 = \tan \frac{A}{2}, \quad t_2 = \tan \frac{B}{2}, \quad t_3 = \tan \frac{C}{2}.$$

These satisfy

$$t_1 t_2 + t_2 t_3 + t_3 t_1 = 1. \quad (10.1)$$



We shall assume throughout this chapter that all sidelengths of triangles are rational. Such a triangle is called a *rational* triangle if its **area** is

rational. Equivalently,  $t_1, t_2, t_3$  are all rational numbers. Putting  $t_i = \frac{n_i}{d_i}$ ,  $i = 1, 2, 3$ , with  $\gcd(n_i, d_i) = 1$ , we rewrite (14.1) in the form

$$n_1n_2d_3 + n_1d_2n_3 + d_1n_2n_3 = d_1d_2d_3. \quad (10.2)$$

A rational triangle, under a suitable magnification, gives a *primitive* Heron triangle, one with integer sides which are relatively prime, and with integer area. In fact, by putting

$$\begin{aligned} a &= n_1(d_2n_3 + n_2d_3), \\ b &= n_2(d_3n_1 + n_3d_1), \\ c &= n_3(d_1n_2 + n_1d_2), \end{aligned} \quad (10.3)$$

we obtain a Heron triangle with semiperimeter  $s = n_1n_2d_3 + n_1d_2n_3 + d_1n_2n_3 = d_1d_2d_3$  and area  $\Delta = n_1d_1n_2d_2n_3d_3$ . A primitive Heron triangle  $\Gamma_0$  results by dividing by the sides by  $g := \gcd(a_1, a_2, a_3)$ .

### 10.1.2 Triple of simplifying factors

Unless explicitly stated otherwise, whenever the three indices  $i, j, k$  appear altogether in an expression or an equation, they are taken as a *permutation* of the indices 1, 2, 3.

Note that from (14.1) or (10.2), any one of  $t_i, t_j, t_k$  can be expressed in terms of the remaining two. In the process of expressing  $t_i = \frac{n_i}{d_i}$  in terms of  $t_j = \frac{n_j}{d_j}$  and  $t_k = \frac{n_k}{d_k}$ , we encounter certain “simplifying factors”, namely,

$$g_i := \gcd(d_jd_k - n_jn_k, n_jd_k + d_jn_k),$$

so that

$$\begin{aligned} g_in_i &= d_jd_k - n_jn_k, \\ g_id_i &= d_jn_k + n_jd_k, \end{aligned} \quad (10.4)$$

We shall call  $(g_1, g_2, g_3)$  the *triple of simplifying factors* for the numbers  $(t_1, t_2, t_3)$ , or of the similarity class of triangles they define.

**Example 10.1.** For the  $(13, 14, 15; 84)$ , we have  $t_1 = \frac{1}{2}$ ,  $t_2 = \frac{4}{7}$  and  $t_3 = \frac{2}{3}$ . From

$$\frac{1 - t_2t_3}{t_2 + t_3} = \frac{7 \cdot 3 - 4 \cdot 2}{7 \cdot 2 + 4 \cdot 3} = \frac{13}{26} = \frac{1}{2},$$

it follows that  $g_1 = 13$ . Similarly,  $g_2 = 1$  and  $g_3 = 5$ . On the other hand, for the indecomposable Heron triangle  $(25, 34, 39; 420)$ , we have  $(t_1, t_2, t_3) = (\frac{5}{14}, \frac{4}{7}, \frac{6}{7})$ . The simplifying factors are  $(g_1, g_2, g_3) = (5, 17, 13)$ .

**Example 10.2.** For  $(15, 34, 35; 252)$ , the simplifying factors are  $(g_1, g_2, g_3) = (5, 17, 5)$ .

### Exercise

For the sidelengths given in (10.3), we have

$$a = g_1 n_1 d_1, \quad b = g_2 n_2 d_2, \quad c = g_3 n_3 d_3.$$

### 10.1.3 Decomposition of Heron triangles

A Heron triangle  $\Gamma := (a_1, a_2, a_3; \Delta)$  is said to be *decomposable* if there are (nondegenerate) Pythagorean triangles  $\Gamma_1 := (x_1, y, a_1; \Delta_1)$ ,  $\Gamma_2 := (x_2, y, a_2; \Delta_2)$ , and  $\epsilon = \pm 1$  such that

$$a_3 = \epsilon x_1 + x_2, \quad \Delta = \epsilon \Delta_1 + \Delta_2.$$

According as  $\epsilon = 1$  or  $-1$ , we shall say that  $\Gamma$  is obtained by juxtaposing  $\Gamma_1$  and  $\Gamma_2$ , ( $\Gamma = \Gamma_1 \cup \Gamma_2$ ), or by excising  $\Gamma_1$  from  $\Gamma_2$ , ( $\Gamma = \Gamma_2 \setminus \Gamma_1$ ).

In general, a Heron triangle is decomposable into two Pythagorean components if and only if it has at least one integer height.

**Theorem 10.1.** *A primitive Heron triangle can be decomposed into two Pythagorean components in at most one way.*

*Proof.* This follows from three propositions.

(1) A primitive Pythagorean triangle is indecomposable.<sup>1</sup>

(2) A primitive, isosceles, Heron triangle is decomposable, the only decomposition being into two congruent Pythagorean triangles.<sup>2</sup>

<sup>1</sup>Proof of (1). We prove this by contradiction. A Pythagorean triangle, if decomposable, is partitioned by the altitude on the hypotenuse into two similar but *smaller* Pythagorean triangles. None of these, however, can have all sides of integer length by the primitivity assumption on the original triangle.

<sup>2</sup>Proof of (2). The triangle being isosceles and Heron, the perimeter and hence the base must be even. Each half of the isosceles triangle is a (primitive) Pythagorean triangle,  $(n^2 - n^2, 2mn, m^2 + n^2)$ , with  $m, n$  relatively prime, and of different parity. The height on each slant side of the isosceles triangle is

$$\frac{2mn(m^2 - n^2)}{m^2 + n^2},$$

which clearly cannot be an integer. This shows that the only way of decomposing a primitive isosceles triangle is into two congruent Pythagorean triangles.

(3) If a non-Pythagorean Heron triangle has two integer heights, then it cannot be primitive.<sup>3</sup>  $\square$

## 10.2 Gaussian integers

We shall associate with each positive rational number  $t = \frac{n}{d}$ ,  $n, d$  relatively prime, the primitive, positive Gaussian integer  $z(t) := d + n\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ . Here, we say that a Gaussian integer  $x + y\sqrt{-1}$  is

- *primitive* if  $x$  and  $y$  are relatively prime, and
- *positive* if both  $x$  and  $y$  are positive.

The norm of the Gaussian integer  $z = x + y\sqrt{-1}$  is the integer  $N(z) := x^2 + y^2$ . The norm in  $\mathbb{Z}[\sqrt{-1}]$  is *multiplicative*:

$$N(z_1 z_2) = N(z_1)N(z_2).$$

The *argument* of a Gaussian integer  $z = x + y\sqrt{-1}$  is the unique real number  $\phi = \phi(z) \in [0, 2\pi)$  defined by

$$\cos \phi = \frac{x}{\sqrt{x^2 + y^2}}, \quad \sin \phi = \frac{y}{\sqrt{x^2 + y^2}}.$$

A Gaussian integer  $z$  is positive if and only if  $0 < \theta(z) < \frac{1}{2}\pi$ . Each positive Gaussian integer  $z = x + y\sqrt{-1}$  has a *complement*

$$z^* := y + x\sqrt{-1} = \sqrt{-1} \cdot \bar{z},$$

---

<sup>3</sup>Proof of (3). Let  $(a, b, c; \Delta)$  be a Heron triangle, not containing any right angle. Suppose the heights on the sides  $b$  and  $c$  are integers. Clearly,  $b$  and  $c$  cannot be relatively prime, for otherwise, the heights of the triangle on these sides are respectively  $ch$  and  $bh$ , for some integer  $h$ . This is impossible since, the triangle not containing any right angle, the height on  $b$  must be less than  $c$ . Suppose therefore  $\gcd(b, c) = g > 1$ . We write  $b = b'g$  and  $c = c'g$  for relatively prime integers  $b'$  and  $c'$ . If the height on  $c$  is  $h$ , then that on the side  $b$  is  $\frac{ch}{b} = \frac{c'h}{b'}$ . If this is also an integer, then  $h$  must be divisible by  $b'$ . Replacing  $h$  by  $b'h$ , we may now assume that the heights on  $b$  and  $c$  are respectively  $c'h$  and  $b'h$ . The side  $c$  is divided into  $b'k$  and  $\pm(c - b'k) \neq 0$ , where  $g^2 = h^2 + k^2$ . It follows that

$$\begin{aligned} a^2 &= (b'h)^2 + (c'g - b'k)^2 \\ &= b'^2(h^2 + k^2) + c'^2g^2 - 2b'c'gk \\ &= g[g(b'^2 + c'^2) - 2b'c'k] \end{aligned}$$

From this it follows that  $g$  divides  $a^2$ , and every prime divisor of  $g$  is a common divisor of  $a, b, c$ . The Heron triangle cannot be primitive.

where  $\bar{z} := x - y\sqrt{-1}$  is the conjugate of  $z$ . Note that  $N(z^*) = N(z)$ , and

$$\phi(z) + \phi(z^*) = \frac{\pi}{2}. \quad (10.5)$$

for each pair of complementary positive Gaussian integers.

Recall that the units of  $\mathbb{Z}[\sqrt{-1}]$  are precisely  $\pm 1$  and  $\pm\sqrt{-1}$ . An odd (rational) prime number  $p$  ramifies into two non - associate primes  $\pi(p)$  and  $\overline{\pi(p)}$  in  $\mathbb{Z}[\sqrt{-1}]$ , namely,  $p = \pi(p)\overline{\pi(p)}$ , if and only if  $p \equiv 1 \pmod{4}$ . For applications in the present paper, we formulate the unique factorization theorem in  $\mathbb{Z}[\sqrt{-1}]$  as follows.

**Proposition 10.2.** *Let  $g > 1$  be an odd number. There is a primitive Gaussian integer  $\theta$  satisfying  $N(\theta) = g$  if and only if each prime divisor of  $g$  is congruent to 1 (mod 4).*

### 10.2.1 Heron triangles and Gaussian integers

Consider the Heron triangle  $\Gamma := \Gamma(t_1, t_2, t_3)$  with sides given by (10.3). In terms of the Gaussian integers  $z_i := z(t_i) = d_i + n_i\sqrt{-1}$ , the relations (10.4) can be rewritten as

$$g_i z_i = \sqrt{-1} \cdot \overline{z_j z_k} = (z_j z_k)^*. \quad (10.6)$$

**Lemma 10.3.**  $N(z_i) = g_j g_k$ .

*Proof.* From the relation (10.6), we have

$$g_i^2 N(z_i) = N(z_j) N(z_k).$$

Combining these, we have

$$(g_i g_j g_k)^2 = N(z_i) N(z_j) N(z_k),$$

and the result follows easily.  $\square$

**Proposition 10.4.** (1)  $g_i$  is a common divisor of  $N(z_j)$  and  $N(z_k)$ .

(2) At least two of  $g_i, g_j, g_k$  exceed 1.

(3)  $g_i$  is even if and only if all  $n_j, d_j, n_k$  and  $d_k$  are odd.

(4) At most one of  $g_i, g_j, g_k$  is even, and none of them is divisible by 4.

(5)  $g_i$  is prime to each of  $n_j, d_j, n_k$ , and  $d_k$ .

(6) Each odd prime divisor of  $g_i, i = 1, 2, 3$ , is congruent to 1 (mod 4).

*Proof.* (1) follows easily from Lemma 10.3.

(2) Suppose  $g_1 = g_2 = 1$ . Then,  $N(z_3) = 1$ , which is clearly impossible.

(3) is clear from the relation (10.4).

(4) Suppose  $g_i$  is even. Then  $n_j, d_j, n_k, d_k$  are all odd. This means that  $g_i$ , being a divisor of  $N(z_j) = d_j^2 + n_j^2 \equiv 2 \pmod{4}$ , is not divisible by 4. Also,  $d_j d_k - n_j n_k$  and  $n_j d_k + d_j n_k$  are both even, and

$$\begin{aligned} & (d_j d_k - n_j n_k) + (n_j d_k + d_j n_k) \\ &= (d_j + n_j)(d_k + n_k) - 2n_j n_k \\ &\equiv 2 \pmod{4}, \end{aligned}$$

it follows that one of them is divisible by 4, and the other is  $2 \pmod{4}$ . After cancelling the common divisor 2, we see that exactly one of  $n_i$  and  $d_i$  is odd. This means, by (c), that  $g_j$  and  $g_k$  cannot be odd.

(5) If  $g_i$  and  $n_j$  admit a common prime divisor  $p$ , then  $p$  divides both  $n_j$  and  $n_j^2 + d_j^2$ , and hence  $d_j$  as well, contradicting the assumption that  $d_j + n_j\sqrt{-1}$  be primitive.

(6) is a consequence of Proposition 10.2.  $\square$

**Proposition 10.5.**  $\gcd(g_1, g_2, g_3) = 1$ .

*Proof.* We shall derive a contradiction by assuming a common rational prime divisor  $p \equiv 1 \pmod{4}$  of  $g_i, g_j, g_k$ , with *positive* exponents  $r_i, r_j, r_k$  in their prime factorizations. By the relation (10.6), the product  $z_j z_k$  is divisible by the *rational* prime power  $p^{r_i}$ . This means that the primitive Gaussian integers  $z_j$  and  $z_k$  should contain in their prime factorizations powers of the distinct primes  $\pi(p)$  and  $\overline{\pi(p)}$ . The same reasoning also applies to each of the pairs  $(z_k, z_i)$  and  $(z_i, z_j)$ , so that  $z_k$  and  $z_i$  (respectively  $z_i$  and  $z_j$ ) each contains one of the non - associate Gaussian primes  $\pi(p)$  and  $\overline{\pi(p)}$  in their factorizations. But then this means that  $z_j$  and  $z_k$  are divisible by the *same* Gaussian prime, a contradiction.  $\square$

**Corollary 10.6.** *If  $a, b, c$  are given as in (10.3), then*

$$\gcd(a, b, c) = \gcd(n_1 d_1, n_2 d_2, n_3 d_3).$$

*Proof.* This follows from the expressions (10.3):  $a_i = g_i n_i d_i$ , for  $i = 1, 2, 3$ , and Proposition 10.5.  $\square$

**Exercise**

Prove that a Heron triangle is Pythagorean if and only if its triple of simplifying factors is of the form  $(1, 2, g)$ , for an odd number  $g$  whose prime divisors are all of the form  $4m + 1$ .

**10.3 Orthocentric Quadrangles**

Now we consider a rational triangle which does not contain a right angle. The vertices and the orthocenter form an orthocentric quadrangle, *i.e.*, each of these four points is the orthocenter of the triangle with vertices at the remaining three points. If any of the four triangles is rational, then so are the remaining three. The convex hull of these four points is an acute - angled triangle  $\Gamma$ . We label the vertices  $A, B, C$ , and the orthocenter in the interior by  $H$  and use the following notation for triangles:

$$\Gamma = ABC, \quad \Gamma_1 = HBC, \quad \Gamma_2 = BHC, \quad \Gamma_3 = ABH.$$

Let  $t_1, t_2, t_3$  be the tangents of the half angles of  $\Gamma$ ,  $z_1, z_2, z_3$  the associated Gaussian integers, and  $(g_1, g_2, g_3)$  the corresponding simplifying factors. Then the tangents of the half angles of  $\Gamma_k$  are

$$\frac{1 - t_i}{1 + t_i}, \quad \frac{1 - t_j}{1 + t_j}, \quad \text{and} \quad \frac{1}{t_k}.$$

We first assume that  $g_1, g_2, g_3$  are all odd, so that for  $i = 1, 2, 3$ ,  $d_i$  and  $n_i$  are of different parity, (Proposition 10.4(3)). The triangle  $\Gamma_k$  has associated primitive Gaussian integers

$$\begin{aligned} z'_i &= (d_i + n_i) + (d_i - n_i)\sqrt{-1} = (1 + \sqrt{-1})z_i, \\ z'_j &= (d_j + n_j) + (d_j - n_j)\sqrt{-1} = (1 + \sqrt{-1})z_j, \\ z'_k &= n_k + d_k\sqrt{-1} = \sqrt{-1} \cdot \bar{z}_k. \end{aligned} \tag{10.7}$$

From these,

$$\begin{aligned} z'_j z'_k &= (1 + \sqrt{-1})\sqrt{-1} \cdot \bar{z}_j \bar{z}_k = g_i(1 + \sqrt{-1})z_i = g_i\sqrt{-1} \cdot \bar{z}'_i, \\ z'_i z'_k &= (1 + \sqrt{-1})\sqrt{-1} \cdot \bar{z}_i \bar{z}_k = g_j(1 + \sqrt{-1})z_j = g_j\sqrt{-1} \cdot \bar{z}'_j, \\ z'_i z'_j &= 2\sqrt{-1} \cdot \bar{z}_i \bar{z}_j = 2g_k z_k = 2g_k\sqrt{-1} \cdot \bar{z}'_k. \end{aligned}$$

Thus, the triangle  $\Gamma_k$  has simplifying factors  $(g_i, g_j, 2g_k)$ .

Suppose now that one of the simplifying factors of  $\Gamma$ , say,  $g_k$  is even. Then  $n_i, d_i, n_j, d_j$  are all odd, and  $n_k, d_k$  have different parity. A similar calculation shows that the simplifying factors for the triangles  $\Gamma_i, \Gamma_j$  and  $\Gamma_k$  are  $(2g_i, g_j, \frac{g_k}{2}), (g_i, 2g_j, \frac{g_k}{2}),$  and  $(g_i, g_j, \frac{g_k}{2})$  respectively.

We summarize these in the following proposition.

**Proposition 10.7.** *The simplifying factors for the four (rational) triangles in an orthocentric quadrangle are of the form  $(g_1, g_2, g_3), (2g_1, g_2, g_3), (g_1, 2g_2, g_3)$  and  $(g_1, g_2, 2g_3)$ , with  $g_1, g_2, g_3$  odd integers.*

## 10.4 Indecomposable primitive Heron triangles

A routine computer search gives the following indecomposable, primitive Heron triangles with sides  $\leq 100$ , excluding Pythagorean triangles:

(5, 29, 30; 72)	(10, 35, 39; 168)	(15, 34, 35; 252)	(13, 40, 45; 252)	(17, 40, 41; 336)
(25, 34, 39; 420)	(5, 51, 52; 126)	(15, 52, 61; 336)	(20, 53, 55; 528)	(37, 39, 52; 720)
(17, 55, 60; 462)	(26, 51, 73; 420)	(17, 65, 80; 288)	(29, 65, 68; 936)	(34, 55, 87; 396)
(39, 55, 82; 924)	(41, 50, 89; 420)	(35, 65, 82; 1092)	(26, 75, 91; 840)	(39, 58, 95; 456)
(17, 89, 90; 756)	(26, 73, 97; 420)	(41, 60, 95; 798)	(51, 52, 97; 840)	

We study the condition under which the primitive Heron triangle  $\Gamma_0 = \Gamma_0(t_1, t_2, t_3)$  constructed in §10.1.1 is *indecomposable*. Clearly,  $\Gamma_0 = \Gamma(t_1, t_2, t_3)$  is indecomposable if this is so for the triangle  $\Gamma$  defined by (10.3). More remarkable is the validity of the converse.

**Theorem 10.8.** *A non-Pythagorean, primitive Heron triangle  $\Gamma_0 = \Gamma_0(t_1, t_2, t_3)$  is indecomposable if and only if each of the simplifying factors  $g_i, i = 1, 2, 3$ , contains an odd prime divisor.*

*Proof.* We first prove the theorem for the triangle  $\Gamma := \Gamma(t_1, t_2, t_3)$  defined by (10.3).

Since  $\Gamma$  has area  $\Delta = n_1d_1n_2d_2n_3d_3$ , the height on the side  $a_i = g_in_id_i$  is given by

$$h_i = \frac{2n_jd_jn_kd_k}{g_i}.$$

Since the triangle does not contain a right angle, it is indecomposable if and only if none of the heights  $h_i, i = 1, 2, 3$ , is an integer. By Proposition 8(d), this is the case if and only if each of  $g_1, g_2, g_3$  contains an odd prime divisor.

To complete the proof, note that the sides (and hence also the heights) of  $\Gamma_0$  are  $\frac{1}{g}$  times those of  $\Gamma$ . Here,  $g := \gcd(a_1, a_2, a_3) = \gcd(n_1d_1, n_2d_2, n_3d_3)$  by Corollary 10.6. The heights of  $\Gamma_0$  are therefore

$$h'_i = \frac{2n_jd_jn_kd_k}{g_i \cdot g} = \frac{2}{g_i} \cdot \frac{n_jd_jn_kd_k}{\gcd(n_1d_1, n_2d_2, n_3d_3)}.$$

Note that  $\frac{n_jd_jn_kd_k}{\gcd(n_1d_1, n_2d_2, n_3d_3)}$  is an integer prime to  $g_i$ . If  $h'_i$  is not an integer, then  $g_i$  must contain an odd prime divisor, by Proposition 10.4(4) again.  $\square$

**Corollary 10.9.** *Let  $\Gamma$  be a primitive Heron triangle. Denote by  $\Gamma_i$ ,  $i = 1, 2, 3$ , the primitive Heron triangles in the similarity classes of the remaining three rational triangles in the orthocentric quadrangle containing  $\Gamma$ . The four triangles  $\Gamma$  and  $\Gamma_i$ ,  $i = 1, 2, 3$ , are either all decomposable or all indecomposable.*

**Example 10.3.** From the orthocentric quadrangle of each the indecomposable Heron triangles (15, 34, 35; 252) and (25, 34, 39; 420), we obtain three other indecomposable primitive Heron triangles.

$(a_1, b_1, c_1)$	$(g_1, g_2, g_3)$	$(a_1, b_1, c_1)$	$(g_1, g_2, g_3)$
(15, 34, 35; 252)	(5, 17, 5)	(25, 34, 39; 420)	(5, 17, 13)
(55, 17, 60; 462)	(5, 17, 10)	(285, 187, 364; 26334)	(5, 17, 26)
(119, 65, 180; 1638)	(5, 17, 10)	(700, 561, 169; 30030)	(10, 17, 13)
(65, 408, 385; 12012)	(5, 34, 5)	(855, 952, 169; 62244)	(5, 34, 13)

### 10.4.1 Construction of Heron triangles with given simplifying factors

**Theorem 10.10.** *Let  $g_1, g_2, g_3$  be odd numbers satisfying the following conditions.*

- (i) *At least two of  $g_1, g_2, g_3$  exceed 1.*
- (ii) *The prime divisors of  $g_i$ ,  $i = 1, 2, 3$ , are all congruent to 1 (mod 4).*
- (iii)  $\gcd(g_1, g_2, g_3) = 1$ .

*Suppose  $g_1, g_2, g_3$  together contain  $\lambda$  distinct rational (odd) prime divisors. Then there are  $2^{\lambda-1}$  distinct, primitive Heron triangles with simplifying factors  $(g_1, g_2, g_3)$ .*

*Proof.* Suppose  $(g_1, g_2, g_3)$  satisfies these conditions. By (ii), there are primitive Gaussian integers  $\theta_i$ ,  $i = 1, 2, 3$ , such that  $g_i = N(\theta_i)$ . Since  $\gcd(g_1, g_2, g_3) = 1$ , if a rational prime  $p \equiv 1 \pmod{4}$  divides  $g_i$  and  $g_j$ , then, in the ring  $\mathbb{Z}[\sqrt{-1}]$ , the prime factorizations of  $\theta_i$  and  $\theta_j$  contain powers of the same Gaussian prime  $\pi$  or  $\bar{\pi}$ .

Therefore, if  $g_1, g_2, g_3$  together contain  $\lambda$  rational prime divisors, then there are  $2^\lambda$  choices of the triple of primitive Gaussian integers  $(\theta_1, \theta_2, \theta_3)$ , corresponding to a choice between the Gaussian primes  $\pi(p)$  and  $\bar{\pi}(p)$  for each of these rational primes. Choose units  $\epsilon_1$  and  $\epsilon_2$  such that  $z_1 = \epsilon_1 \theta_2 \bar{\theta}_3$  and  $z_2 = \epsilon_2 \theta_3 \bar{\theta}_1$  are positive.

Two positive Gaussian integers  $z_1$  and  $z_2$  define a positive Gaussian integer  $z_3$  via (10.6) if and only if

$$0 < \phi(z_1) + \phi(z_2) < \frac{\pi}{2}. \quad (10.8)$$

Since  $\phi(z_1^*) + \phi(z_2^*) = \pi - (\phi(z_1) + \phi(z_2))$ , it follows that exactly one of the two pairs  $(z_1, z_2)$  and  $(z_1^*, z_2^*)$  satisfies condition (10.8). There are, therefore,  $2^{\lambda-1}$  Heron triangles with  $(g_1, g_2, g_3)$  as simplifying factors.  $\square$

Making use of Theorems 10.8, 10.10, and Proposition 10.7, it is now easy to construct indecomposable primitive Heron triangles from any triples of odd integers  $(g_1, g_2, g_3)$ , each greater than 1, and satisfying the conditions of Theorem 10.10. For example, by choosing  $g_1, g_2, g_3$  from the first few primes of the form  $4k + 1$ , we obtain the following primitive Heron triangles, all indecomposable:

$(g_1, g_2, g_3)$	$(d_1, n_1)$	$(d_2, n_2)$	$(d_3, n_3)$	$(a, b, c; \Delta)$
(5, 13, 17)	(14, 5)	(7, 6)	(7, 4)	(25, 39, 34; 420)
	(5, 14)	(9, 2)	(8, 1)	(175, 117, 68; 2520)
	(11, 10)	(7, 6)	(8, 1)	(275, 273, 68; 9240)
	(10, 11)	(9, 2)	(7, 4)	(275, 117, 238; 13860)
(5, 13, 29)	(4, 19)	(12, 1)	(8, 1)	(95, 39, 58; 456)
	(16, 11)	(8, 9)	(8, 1)	(110, 117, 29; 1584)
	(11, 16)	(12, 1)	(7, 4)	(220, 39, 203; 3696)
	(19, 4)	(8, 9)	(7, 4)	(95, 234, 203; 9576)
(5, 17, 29)	(22, 3)	(12, 1)	(2, 9)	(55, 34, 87; 396)
	(18, 13)	(9, 8)	(9, 2)	(65, 68, 29; 936)
	(18, 13)	(12, 1)	(6, 7)	(195, 34, 203; 3276)
	(22, 3)	(9, 8)	(7, 6)	(55, 204, 203; 5544)
(13, 17, 29)	(22, 3)	(16, 11)	(10, 11)	(39, 136, 145; 2640)
	(22, 3)	(19, 4)	(5, 14)	(429, 646, 1015; 87780)
	(18, 13)	(19, 4)	(11, 10)	(1521, 646, 1595; 489060)
	(18, 13)	(16, 11)	(14, 5)	(1521, 1496, 1015; 720720)

Further examples can be obtained by considering the orthocentric quadrangle of each of these triangles.

# Chapter 11

## Infinite continued fractions

Associated with an infinite continued fraction  $[q_0, q_1, q_2, q_3, \dots, q_n, \dots]$  is a sequence of *convergents* which are finite continued fractions:

$$\frac{P_k}{Q_k} = [q_0, q_1, \dots, q_k].$$

The numerators  $P_k$  and  $Q_k$  can be determined recursively as follows.

$$\begin{aligned} P_k &= P_{k-2} + q_k P_{k-1}, & P_{-2} &= 0, & P_{-1} &= 1, \\ Q_k &= Q_{k-2} + q_k Q_{k-1}, & Q_{-2} &= 1, & Q_{-1} &= 0. \end{aligned}$$

### Examples

1. The successive convergents of the continued fraction  $[1, 2, 3, 4, 5, 6, 7, 8, 9, 10]$  are computed easily using these relations.

$k$	-2	-1	0	1	2	3	4	5	6	7	8	9
$q_k$			1	2	3	4	5	6	7	8	9	10
$P_k$	0	1	1	3	10	43	225	1393	9976	81201	740785	7489051
$Q_k$	1	0	1	2	7	30	157	972	6961	56660	516901	5225670

2. Here are the convergents of the continued fraction  $[1, 2, 1, 3, 1, 4, 1, 5, 1, 6]$  and their differences:

$$\begin{array}{cccccccccc} 1 & \frac{3}{2} & \frac{4}{3} & \frac{15}{11} & \frac{19}{14} & \frac{91}{67} & \frac{110}{81} & \frac{641}{472} & \frac{751}{553} & \frac{5147}{3790} \\ & \frac{1}{2} & \frac{-1}{6} & \frac{1}{33} & \frac{-1}{154} & \frac{1}{938} & \frac{-1}{5427} & \frac{1}{38232} & \frac{-1}{261016} & \frac{1}{2095870} \end{array}$$

Note that the numerators of the differences are all  $\pm 1$ .

**Lemma 11.1.**  $\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^{k-1}}{Q_{k-1}Q_k}$ .

*Proof.* Write  $\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{N_k}{Q_{k-1}Q_k}$ . We have

$$\begin{aligned} N_k &= P_k Q_{k-1} - Q_k P_{k-1} \\ &= (P_{k-2} + q_k P_{k-1}) Q_{k-1} - (Q_{k-2} + q_k Q_{k-1}) P_{k-1} \\ &= -(P_{k-1} Q_{k-2} - Q_{k-1} P_{k-2}) \\ &= -N_{k-1}. \end{aligned}$$

Since  $N_1 = 1$ , we have by easy induction  $N_k = (-1)^{k-1} N_1 = (-1)^{k-1}$ , and the result follows.  $\square$

**Theorem 11.2.** *Let  $q_0, q_1, \dots, q_n, \dots$  be an infinite sequence of positive integers,  $q_0$  possibly zero. The infinite continued fraction*

$$a := [q_0, q_1, q_2, \dots, q_n, \dots]$$

*is always well defined, i.e.,  $\lim_{n \rightarrow \infty} [q_0, q_1, \dots, q_n]$  exists. This limit is always an irrational number.*

*Proof.* For each  $n \geq 0$ , let  $a_n$  be the  $n$ -th convergent  $\frac{P_n}{Q_n}$ . By the above lemma,

$$a_{n+2} - a_n = (a_{n+2} - a_{n+1}) + (a_{n+1} - a_n) = \frac{(-1)^{n+1}}{Q_{n+1}Q_n} + \frac{(-1)^n}{Q_n Q_{n-1}} = \frac{(-1)^n (Q_{n+1} - Q_{n-1})}{Q_{n-1}Q_n Q_{n+1}}.$$

Note that  $(Q_n)$  is an increasing sequence of positive integers, (this is clear from the recurrence relation for  $Q_n$ ). It follows that  $a_0, a_2, a_4, \dots$  is an *increasing* sequence, and  $a_1, a_3, a_5, \dots$  is a *decreasing* sequence. Furthermore, each  $a_{2h+1}$  is greater than every  $a_{2k}$ :

$$a_0 < a_2 < a_4 < \dots < a_{2k} < \dots < a_{2h+1} < a_5 < a_3 < a_1.$$

It follows that the subsequences  $a_{2n}$  and  $a_{2n+1}$  are convergent; indeed, they converge to a common limit since

$$\lim_{n \rightarrow \infty} a_{2n+1} - \lim_{n \rightarrow \infty} a_{2n} = \lim_{n \rightarrow \infty} (a_{2n+1} - a_{2n}) = \lim_{n \rightarrow \infty} \frac{1}{Q_{2n} Q_{2n+1}} = 0$$

since the sequence  $(Q_n)$  of *positive integers* is strictly increasing. The common limit  $a$  of these two subsequences is the *infinite* continued fraction  $[q_0, q_1, \dots, q_n, \dots]$ . This number  $a$  is *irrational* since its continued fraction expansion is not finite.  $\square$

Let  $\zeta$  be a real, irrational number, The continued fraction expansion of  $\zeta$  can be found recursively as follows.

$$\zeta_0 = \zeta, \quad q_0 = [\zeta_0]; \quad \zeta_{n+1} = \frac{1}{\zeta_n - [\zeta_n]}, \quad q_{n+1} = [\zeta_{n+1}].$$

Then,

$$\zeta = [q_0, q_1, q_2, \dots, q_n, \dots].$$

**Theorem 11.3 (Lagrange).** *Let  $d$  be a nonsquare integer. The continued fraction expansion of a quadratic irrationality of the form  $a + b\sqrt{d}$ ,  $a, b \in \mathbb{Q}$ , is eventually periodic; i.e., there exist  $k$  and  $l$  such that in the expansion*

$$a + b\sqrt{d} = [q_0, q_1, \dots, q_n, \dots],$$

$$q_{k+nl+i} = q_{k+i} \text{ for } n \geq 0, 0 \leq i < l.$$

**Theorem 11.4.** *Let  $d$  be a rational number which is not a square. The continued fraction expansion of  $\sqrt{d}$  is of the form*

$$\sqrt{d} = [q_0, \overline{q_1, q_2, \dots, q_2, q_1, 2q_0}],$$

$$\text{where } q_0 = [\sqrt{d}].$$

### Examples

1. Continued fraction expansions of  $\sqrt{d}$ ,  $d < 50$ . Those with asterisks have periods of *odd* lengths.

$\sqrt{2}^*$	=	$[1, \overline{2}];$	$\sqrt{27}$	=	$[5, \overline{5, 10}];$
$\sqrt{3}$	=	$[1, 1, \overline{2}];$	$\sqrt{28}$	=	$[5, 3, 2, 3, \overline{10}];$
$\sqrt{5}^*$	=	$[2, \overline{4}];$	$\sqrt{29}^*$	=	$[5, 2, 1, 1, 2, \overline{10}];$
$\sqrt{6}$	=	$[2, 2, \overline{4}];$	$\sqrt{30}$	=	$[5, 2, \overline{10}];$
$\sqrt{7}$	=	$[2, 1, 1, 1, \overline{4}];$	$\sqrt{31}$	=	$[5, 1, 1, 3, 5, 3, 1, 1, \overline{10}];$
$\sqrt{8}$	=	$[2, 1, \overline{4}];$	$\sqrt{32}$	=	$[5, 1, 1, 1, \overline{10}];$
$\sqrt{10}^*$	=	$[3, \overline{6}];$	$\sqrt{33}$	=	$[5, 1, 2, 1, \overline{10}];$
$\sqrt{11}$	=	$[3, 3, \overline{6}];$	$\sqrt{34}$	=	$[5, 1, 4, 1, \overline{10}];$
$\sqrt{12}$	=	$[3, 2, \overline{6}];$	$\sqrt{35}$	=	$[5, 1, \overline{10}];$
$\sqrt{13}^*$	=	$[3, 1, 1, 1, 1, \overline{6}];$	$\sqrt{37}^*$	=	$[6, \overline{12}];$
$\sqrt{14}$	=	$[3, 1, 2, 1, \overline{6}];$	$\sqrt{38}$	=	$[6, 6, \overline{12}];$
$\sqrt{15}$	=	$[3, 1, \overline{6}];$	$\sqrt{39}$	=	$[6, 4, \overline{12}];$
$\sqrt{17}^*$	=	$[4, \overline{8}];$	$\sqrt{40}$	=	$[6, 3, \overline{12}];$
$\sqrt{18}$	=	$[4, 4, \overline{8}];$	$\sqrt{41}^*$	=	$[6, 2, 2, \overline{12}];$
$\sqrt{19}$	=	$[4, 2, 1, 3, 1, 2, \overline{8}];$	$\sqrt{42}$	=	$[6, 2, \overline{12}];$
$\sqrt{20}$	=	$[4, 2, \overline{8}];$	$\sqrt{43}$	=	$[6, 1, 1, 3, 1, 5, 1, 3, 1, 1, \overline{12}];$
$\sqrt{21}$	=	$[4, 1, 1, 2, 1, 1, \overline{8}];$	$\sqrt{44}$	=	$[6, 1, 1, 1, 2, 1, 1, 1, \overline{12}];$
$\sqrt{22}$	=	$[4, 1, 2, 4, 2, 1, \overline{8}];$	$\sqrt{45}$	=	$[6, 1, 2, 2, 2, 1, \overline{12}];$
$\sqrt{23}$	=	$[4, 1, 3, 1, \overline{8}];$	$\sqrt{46}$	=	$[6, 1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, \overline{12}];$
$\sqrt{24}$	=	$[4, 1, \overline{8}];$	$\sqrt{47}$	=	$[6, 1, 5, 1, \overline{12}];$
$\sqrt{26}^*$	=	$[5, \overline{10}];$	$\sqrt{48}$	=	$[6, 1, \overline{12}].$

2. Some simple patterns:

$$\begin{aligned}\sqrt{a^2 + 1} &= [a, \overline{a, 2a}]; \\ \sqrt{a^2 - 1} &= [a - 1, \overline{1, 2a - 2}]; \\ \sqrt{a^2 + a} &= [a, \overline{2, 2a}]; \\ \sqrt{a^2 + 2} &= [a, \overline{a, 2a}]; \\ \sqrt{a^2 - 2} &= [a - 1, \overline{1, a - 2, 1, 2a - 2}].\end{aligned}$$

## 11.1 Lagrange's Theorem

### 11.1.1 Purely periodic continued fractions.

Let  $a$  be represented by a *purely periodic* continued fraction:

$$\zeta = [\overline{q_0, q_1, \dots, q_k}].$$

This means  $\zeta = [q_0, q_1, \dots, q_k, \zeta]$ . Let  $\frac{P_{k-1}}{Q_{k-1}}$  and  $\frac{P_k}{Q_k}$  be the last two convergents of the finite continued fraction  $[q_0, q_1, \dots, q_k]$ . Then,

$$\zeta = \frac{P_{k-1} + \zeta P_k}{Q_{k-1} + \zeta Q_k}.$$

From this, we see that  $\zeta$  is a root of the quadratic equation

$$Q_k x^2 - (P_k - Q_{k-1})x - P_{k-1} = 0.$$

Since the product of the two roots of this equation, being  $-\frac{P_{k-1}}{Q_k}$ , is negative, exactly one of them is positive. This must be the number  $\zeta$ , and it is clear that this is a number of the form  $a + b\sqrt{d}$ ,  $a, b \in \mathbb{Q}$ . Here,  $d$  cannot be a square, for otherwise, the number  $\zeta$  would have been rational.

### 11.1.2 Eventually periodic continued fractions

It follows that a number with *eventually periodic* continued fraction expansion is also a quadratic irrationality. Consider

$$\mu = [p_0, p_1, \dots, p_h, \overline{q_1, \dots, q_k}].$$

Let  $\zeta$  be the irrational number with *purely periodic* continued fraction expansion  $[q_1, \dots, q_k]$ . This is of the form  $a + b\sqrt{d}$  according to §11.1.1. If  $h = 0$ , then

$$\mu = [p_0, \zeta] = p_0 + \frac{1}{\zeta}$$

is clearly of the form  $a' + b'\sqrt{d}$ ,  $a', b' \in \mathbb{Q}$ . If  $h \geq 1$ , let  $\frac{P'}{Q'}$  and  $\frac{P}{Q}$  be the last two convergents of the continued fraction  $[p_0, \dots, p_h]$ . Then

$$\mu = [p_0, \dots, p_h, \zeta] = \frac{P' + \zeta P}{Q' + \zeta Q}.$$

This also is of the form  $a' + b'\sqrt{d}$ ,  $a', b' \in \mathbb{Q}$ .

We have therefore proved the easier half of Lagrange theorem: every eventually periodic continued fraction represents a quadratic irrationality. The proof of the converse is more difficult, and requires a more detailed analysis of numbers with purely periodic continued fraction expansions.

### 11.1.3 Reduced quadratic irrationalities

Let  $\zeta = \overline{[q_0, q_1, \dots, q_k]}$ . It is the positive root of the quadratic equation

$$x = [q_0, q_1, \dots, q_k, x].$$

Note that  $q_0 - x = \frac{-1}{[q_1, \dots, q_k, x]}$ , and this can be rewritten as

$$\left[ q_0, \frac{-1}{x} \right] = \frac{-1}{[q_1, \dots, q_k, x]}.$$

Continuing, we obtain

$$\left[ q_k, q_{k-1}, \dots, q_1, q_0, \frac{-1}{x} \right] = \frac{-1}{x}.$$

This means  $\zeta$  is the positive root of  $x = [q_0, q_1, \dots, q_k, x]$  if and only if  $\frac{-1}{\zeta}$  is the positive root of  $y = [q_k, q_{k-1}, \dots, q_0, y]$ . Consequently, it follows that every equation of the form  $x = [q_0, \dots, q_k, x]$  has exactly one positive root  $\zeta > 1$ , and one negative root between  $-1$  and  $0$ . This negative root is necessarily the *conjugate*  $\bar{\zeta}$ . We shall say that a quadratic irrationality  $\zeta$  is *reduced* if it satisfies the condition

$$\zeta > 1 > 0 > \bar{\zeta} > -1.$$

We may paraphrase the conclusion by saying that *a purely periodic continued fraction represents a reduced quadratic irrationality*.

### 11.1.4 Proof of Lagrange's theorem

Consider now a general quadratic irrationality of the form

$$\zeta = \frac{P + \sqrt{d}}{Q},$$

where  $P$ ,  $Q$  and  $d$  are integers. By replacing  $P$ ,  $Q$  and  $d$  by suitable integer multiples, we may assume that  $\frac{d-P^2}{Q}$  is an integer, and we shall work with this assumption, and write  $d = P^2 + QQ'$  for an integer  $Q'$ .

**Lemma 11.5.** *If the quadratic irrationality  $\zeta = \frac{P+\sqrt{d}}{Q}$  is reduced, then the integers  $P$  and  $Q$  are positive, and*

$$P < [\sqrt{d}], \quad Q < P + \sqrt{d} < [2\sqrt{d}].$$

Now, let  $\zeta = \frac{P+\sqrt{d}}{Q}$  be a quadratic irrationality with  $d - P^2 = QQ'$  for some integer  $Q'$ . For every integer  $m$ ,

$$\frac{1}{\zeta - m} = \frac{Q}{P - mQ + \sqrt{d}} = \frac{Q(-P + mQ + \sqrt{d})}{d - (P - mQ)^2} = \frac{-P + mQ + \sqrt{d}}{\frac{1}{Q}[d - (P - mQ)^2]} = \frac{-P + mQ + \sqrt{d}}{Q' + 2mP - m^2Q}.$$

Note that in this expression,

$$d - (P - mQ)^2 = (d - P^2) + 2mPQ - m^2Q^2 = Q(Q' + 2mP - m^2Q).$$

It follows that we can obtain the continued fraction expansion of  $\zeta$  by working out

$$P_0 = P, \quad Q_0 = Q, \quad Q_{-1} = Q',$$

$$\zeta_k = \frac{P_k + \sqrt{d}}{Q_k}, \quad q_k = [\zeta_k],$$

$$P_{k+1} = -P_k + q_k Q_k,$$

$$Q_{k+1} = Q_{k-1} + 2q_k P_k - q_k^2 Q_k = \frac{d - P_{k+1}^2}{Q_k}.$$

Note that  $\zeta = [q_0, \dots, q_{n-1}, \zeta_n]$ . In particular,

$$\zeta = \frac{P_{n-2} + \zeta_n P_{n-1}}{Q_{n-2} + \zeta_n Q_{n-1}}.$$

Consider the conjugate

$$\bar{\zeta} = \frac{P_{n-2} + \bar{\zeta}_n P_{n-1}}{Q_{n-2} + \bar{\zeta}_n Q_{n-1}}.$$

From this,

$$\bar{\zeta}_n = -\frac{Q_{n-2}\bar{\zeta} - P_{n-2}}{Q_{n-1}\bar{\zeta} - P_{n-1}} = -\frac{Q_{n-2}}{Q_{n-1}} \cdot \frac{\bar{\zeta} - \frac{P_{n-2}}{Q_{n-2}}}{\bar{\zeta} - \frac{P_{n-1}}{Q_{n-1}}}.$$

Since the sequence  $\frac{P_n}{Q_n}$  converges to  $\zeta$ , we can choose  $N$  large enough so that  $\bar{\zeta}_N$  lies between  $-1$  and  $0$ . In other words,  $\zeta_N$  is reduced.

It follows as a consequence of this observation that in the construction of the continued fraction expansion of  $\zeta$  above, all  $\zeta_n$ ,  $n \geq N$ , are reduced. By Lemma 11.5, we have

$$0 < P_n < \sqrt{d}, \quad 0 < Q_n < 2\sqrt{d}, \quad \text{for every } n \geq N.$$

There must exist distinct integers  $h, k \geq N$  such that

$$P_h = P_k, \quad Q_h = Q_k.$$

If we choose  $h$  and  $k = h + r$  to be the *smallest* possible integers for which these hold, then for every integer  $t \geq 0$  and  $0 \leq s < r$ ,

$$P_{h+tr+s} = P_{h+s}, \quad Q_{h+tr+s} = Q_{h+s}.$$

From this,

$$q_{h+tr+s} = q_{h+s}.$$

This completes the proof of Lagrange's theorem.

**Corollary 11.6.** *The continued fraction expansion of a reduced quadratic irrationality is purely periodic.*

*Proof.* It is enough to show that if  $\zeta = [q_0, \overline{q_1, \dots, q_r}]$  is reduced, then indeed,  $q_0 = q_r$ . (The general case follows by induction). Let  $\theta = [\overline{q_1, \dots, q_r}]$ . Since  $q_0 + \frac{1}{\theta}$  is reduced,

$$q_0 + \frac{1}{\theta} > 1 > 0 > q_0 + \frac{1}{\bar{\theta}} > -1.$$

From this,  $q_0 = [-\frac{1}{\bar{\theta}}]$ . However,  $-\frac{1}{\bar{\theta}}$  has continued fraction expansion  $[\overline{q_r, \dots, q_1}]$ . It follows that  $q_r = q_0$ .  $\square$

## Exercise

1. If  $x$  is reduced, then so is  $\frac{1}{x-[x]}$ .
2. If a quadratic irrationality  $\zeta > 1$  satisfies  $\bar{\zeta} < -1$ , then the continued fraction expansion of  $\zeta$  has one single term before the period.<sup>1</sup>

---

<sup>1</sup>Solution. There is a positive integer  $c$  such that  $c + \bar{\zeta}$  lies between  $-1$  and  $0$ . In other words,  $c + \zeta$  is reduced, and has periodic continued fraction expansion  $\overline{[q_1, \dots, q_r]}$ . Then,

$$\zeta = [q_1 - c, \overline{q_2, \dots, q_r, q_r}].$$

## Chapter 12

# The Pell Equation

### 12.1 The equation $x^2 - dy^2 = 1$

Let  $d$  be a fixed integer. We consider the *Pell equation*  $x^2 - dy^2 = 1$ . Clearly, if  $d$  is negative or is a (positive) square integer, then the equation has only finitely many solutions.

**Theorem 12.1.** *Let  $d$  be a nonsquare, positive integer. The totality of positive solutions of the Pell equation  $x^2 - dy^2 = 1$  form an infinite sequence  $(x_n, y_n)$  defined recursively by*

$$\begin{aligned}x_{n+1} &= ax_n + dby_n, \\y_{n+1} &= bx_n + ay_n; \quad x_1 = a, \quad y_1 = b,\end{aligned}$$

where  $(x_1, y_1) = (a, b)$  is the fundamental solution (with  $a, b$  smallest possible) obtained from the continued fraction expansion

$$\sqrt{d} = [q_0, \overline{q_1, \dots, q_k}],$$

as follows. Let  $\frac{P_{k-1}}{Q_{k-1}}$  the  $(k-1)$ -th convergent of  $\sqrt{d}$ .

(a). If the length of the period is even, then  $(a, b) = (P_{k-1}, Q_{k-1})$  is the smallest positive solution of the Pell equation  $x^2 - dy^2 = 1$ .

(b). If the length of the period is odd, then the smallest positive solution of the equation  $x^2 - dy^2 = 1$  is  $(a, b) = (P_{k-1}^2 + dQ_{k-1}^2, 2P_{k-1}Q_{k-1})$ .

### Examples

1. The fundamental solution of the Pell equation  $x^2 - 2y^2 = 1$  is  $(3, 2)$ . This generates an infinite sequence of nonnegative solutions

$(x_n, y_n)$  defined by

$$x_{n+1} = 3x_n + 4y_n, \quad y_{n+1} = 2x_n + 3y_n; \quad x_0 = 1, y_0 = 0.$$

The beginning terms are

$n$	1	2	3	4	5	6	7	8	9	10...
$x_n$	3	17	99	577	3363	19601	114243	665857	3880899	22619537 ...
$y_n$	2	12	70	408	2378	13860	80782	470832	2744210	15994428 ...

## 2. Fundamental solution $(a, b)$ of $x^2 - dy^2 = 1$ for $d < 100$ :

$d$	$a$	$b$	$d$	$a$	$b$	$d$	$a$	$b$
2	3	2	3	2	1	5	9	4
6	5	2	7	8	3	8	3	1
10	19	6	11	10	3	12	7	2
13	649	180	14	15	4	15	4	1
17	33	8	18	17	4	19	170	39
20	9	2	21	55	12	22	197	42
23	24	5	24	5	1	26	51	10
27	26	5	28	127	24	29	9801	1820
30	11	2	31	1520	273	32	17	3
33	23	4	34	35	6	35	6	1
37	73	12	38	37	6	39	25	4
40	19	3	41	2049	320	42	13	2
43	3482	531	44	199	30	45	161	24
46	24335	3588	47	48	7	48	7	1
50	99	14	51	50	7	52	649	90
53	66249	9100	54	485	66	55	89	12
56	15	2	57	151	20	58	19603	2574
59	530	69	60	31	4	61	1766319049	226153980
62	63	8	63	8	1	65	129	16
66	65	8	67	48842	5967	68	33	4
69	7775	936	70	251	30	71	3480	413
72	17	2	73	2281249	267000	74	3699	430
75	26	3	76	57799	6630	77	351	40
78	53	6	79	80	9	80	9	1
82	163	18	83	82	9	84	55	6
85	285769	30996	86	10405	1122	87	28	3
88	197	21	89	500001	53000	90	19	2
91	1574	165	92	1151	120	93	12151	1260
94	2143295	221064	95	39	4	96	49	5
97	62809633	6377352	98	99	10	99	10	1

## 3. Pell's equations whose fundamental solutions are very large:

$d$	$a$	$b$
421	3879474045914926879468217167061449	189073995951839020880499780706260
541	3707453360023867028800645599667005001	159395869721270110077187138775196900
601	38902815462492318420311478049	1586878942101888360258625080
613	464018873584078278910994299849	18741545784831997880308784340
661	16421658242965910275055840472270471049	638728478116949861246791167518480580
673	4765506835465395993032041249	183696788896587421699032600
769	53578186838881310859702308423201	19320788325040337217824455505160
919	4481603010937119451551263720	147834442396536759781499589
937	480644425002415999597113107233	15701968936415353889062192632
949	609622436806639069525576201	19789181711517243032971740
991	379516400906811930638014896080	12055735790331359447442538767

4. The equation  $x^2 - 4729494y^2 = 1$  arises from the famous *Cattle problem* of Archimedes, and has *smallest* positive solution

$$\begin{aligned}x &= 109931986732829734979866232821433543901088049, \\y &= 50549485234315033074477819735540408986340.\end{aligned}$$

### Exercise

- Solve the Pell equations (a)  $x^2 + 3y^2 = 1$ ; (b)  $x^2 - 4y^2 = 1$  for *integer* solutions.<sup>1</sup>
- Find the 10 *smallest* nonnegative solutions of the Pell equation  $x^2 - 3y^2 = 1$ .<sup>2</sup>
- For a positive, *nonsquare* integer  $n$ , let  $(a_n, b_n)$  be the fundamental solution of the Pell equation  $x^2 - ny^2 = 1$ . If  $n$  is a square, set  $b_n = 0$ .
  - Show that every positive integer occurs infinitely often in the sequence  $(b_n)$ .
  - Determine all occurrences of  $p^k$ ,  $p$  prime,  $k > 0$ , in the sequence  $(b_n)$ .
- Deduce that if  $p$  is a prime of the form  $4k + 1$ , then the continued fraction expansion of  $\sqrt{p}$  has *odd* period.

#### 12.1.1

If  $(a, b)$  is the *fundamental* solution of the Pell equation  $x^2 - dy^2 = 1$ , generating the infinite sequence of *nonnegative* solutions  $(x_0, y_0) = (1, 0)$ ,  $(x_1, y_1) = (a, b)$ ,  $(x_2, y_2)$ ,  $\dots$ ,  $(x_n, y_n)$ ,  $\dots$ , then

$$x_{n+1} = 2ax_n - x_{n-1}; \quad y_{n+1} = 2ay_n - y_{n-1}.$$

<sup>1</sup>(a).  $(x, y) = (\pm 1, 0)$ ; (b).  $(x, y) = (\pm 1, 0)$ .

$n$	1	2	3	4	5	6	7	8	9	10	11	...
$x_n$	2	7	26	97	362	1351	5042	18817	70226	262087	978122	...
$y_n$	1	4	15	56	209	780	2911	10864	40545	151316	564719	...

## 12.2 The equation $x^2 - dy^2 = -1$

Indeed, if the length of the period of the continued fraction expansion of  $\sqrt{d}$  is odd, then  $(P_{k-1}, Q_{k-1})$  is the *smallest* positive solution of the equation

$$x^2 - dy^2 = -1.$$

Only when this period is odd does this equation have solutions.

### Examples

1. Smallest positive solution  $(a, b)$  of  $x^2 - dy^2 = -1$  for the first 24 values of  $d$ :

$d$	$a$	$b$	$d$	$a$	$b$	$d$	$a$	$b$
2	1	1	5	2	1	10	3	1
13	18	5	17	4	1	26	5	1
29	70	13	37	6	1	41	32	5
50	7	1	53	182	25	58	99	13
61	29718	3805	65	8	1	73	1068	125
74	43	5	82	9	1	85	378	41
89	500	53	97	5604	569	101	10	1

2. If  $p \equiv 1 \pmod{4}$  is prime, then the equation  $x^2 - py^2 = -1$  is solvable.

*Proof.* Let  $(a, b)$  be the fundamental solution of  $x^2 - py^2 = 1$ . This means  $a^2 - 1 = pb^2$ . Note that  $a$  must be odd, for otherwise  $a^2 - 1 \equiv -1 \pmod{4}$ , but  $pb^2 \equiv 1 \pmod{4}$ , a contradiction. Consequently,  $\gcd(a+1, a-1) = 2$ , and we have

(i)  $a+1 = 2r^2$ ,  $a-1 = 2ps^2$ , or

(ii)  $a+1 = 2pr^2$ ,  $a-1 = 2s^2$ , for some nonnegative integers  $r$  and  $s$ .

In (i), we have  $r^2 - ps^2 = 1$ , with  $r < a$ , a contradiction since  $(a, b)$  is the *smallest* positive solution of  $x^2 - py^2 = 1$ . It follows that (ii) holds, and we have  $s^2 - pr^2 = -1$ .  $\square$

## 12.3 The equation $x^2 - dy^2 = c$

Let  $d$  be a *nonsquare* integer, and  $c$  an integer other than  $0, \pm 1$ . Clearly, the equation

$$x^2 - dy^2 = c$$

is solvable only if  $d$  is a quadratic residue modulo  $c$  (**Exercise**). This condition, however, is not sufficient to guarantee existence of solutions. Consider the continued fraction expansion of  $\sqrt{d}$ :

$$\sqrt{d} = [q_0, \overline{q_1, \dots, q_k}],$$

with the first  $k$  convergents

$$\frac{P_i}{Q_i} = [q_0, q_1, \dots, q_i], \quad i = 0, 1, 2, \dots, k - 1.$$

**Theorem 12.2.** *If  $|c| < \sqrt{d}$ , and  $x^2 - dy^2 = c$  is solvable, then  $c$  must be one of the numbers  $P_i^2 - dQ_i^2$ ,  $i = 0, 1, 2, \dots, k - 1$ .*

**Theorem 12.3.** *Let  $c > 1$  be a positive integer.*

(a) *If the equation  $x^2 - dy^2 = c$  is solvable, it must have a fundamental solution  $(u, v)$  in the range*

$$0 < |u| \leq \sqrt{\frac{1}{2}(a+1)c}, \quad 0 \leq v \leq \frac{b}{\sqrt{2(a+1)}} \cdot \sqrt{c}.$$

*Every solution appears in a doubly infinite sequence  $(x_n, y_n)$*

$$\begin{aligned} u_{n+1} &= au_n + dbv_n, \\ v_{n+1} &= bu_n + av_n, \quad u_1 = u, v_1 = v, \end{aligned}$$

*for some  $(u, v)$  in the range above.*

(b) *Same conclusion for the equation  $x^2 - dy^2 = -c$ , except that it must have a solution  $(u, v)$  in the range*

$$0 \leq |u| \leq \sqrt{\frac{1}{2}(a-1)c}, \quad 0 < v \leq \frac{b}{\sqrt{2(a-1)}} \cdot \sqrt{c}.$$

**Example 12.1.** Consider the equation  $x^2 - 23y^2 = 4 \cdot 11 \cdot 23$ . It is easy to see that  $x$  and  $y$  must be both even, and 23 divides  $x$ . With  $x = 46h$ ,  $y = 2k$ , we have  $23h^2 - k^2 = 11$ , or  $k^2 - 23h^2 = -11$ . The fundamental solution of  $x^2 - 23y^2 = 1$  being  $(a, b) = (24, 5)$ , we need only find  $y$  in the range  $1 \leq h \leq 2$ . It is now easy to see that *only*  $h = 2$  gives  $k = 9$ . From this we obtain  $(x_1, y_1) = (92, 18)$ . The other solutions are generated recursively by

$$x_{n+1} = 24x_n + 115y_n, \quad y_{n+1} = 5x_n + 24y_n, \quad x_1 = 92, y_1 = 18.$$

Here are the first 5 solutions.

$n$	1	2	3	4	5	...
$x_n$	92	4278	205252	9847818	472490012	...
$y_n$	18	892	42798	2053412	98520978	...

## 12.4 Applications

1. Which triangular numbers are squares? Suppose the  $k$ -th triangular number  $T_k = \frac{1}{2}k(k+1)$  is the square of  $n$ .  $n^2 = \frac{1}{2}k(k+1)$ ;  $4k^2 + 4k + 1 = 8n^2 + 1$ ;  $(2k+1)^2 - 8n^2 = 1$ . The smallest positive solution of the Pell equation  $x^2 - 8y^2 = 1$  being  $(3, 1)$ , we have the solutions  $(k_i, n_i)$  of the equation given by

$$\begin{aligned} 2k_{i+1} + 1 &= 3(2k_i + 1) + 8n_i, \\ n_{i+1} &= (2k_i + 1) + 3n_i, \quad k_0 = 1, n_0 = 1. \end{aligned}$$

This means

$$\begin{aligned} k_{i+1} &= 3k_i + 4n_i + 1, \\ n_{i+1} &= 2k_i + 3n_i + 1, \quad k_0 = 1, n_0 = 1. \end{aligned}$$

The beginning values of  $k$  and  $n$  are as follows.

$i$	0	1	2	3	4	5	6	7	8	9	10	...
$k_i$	1	8	49	288	1681	9800	57121	332928	1940449	11309768	65918161	...
$n_i$	1	6	35	204	1189	6930	40391	235416	1372105	7997214	46611179	...

2. Find all integers  $n$  so that the mean and the standard deviation of  $n$  consecutive integers are both integers.

If the mean of  $n$  consecutive integers is an integer,  $n$  must be odd. We may therefore assume the numbers to be  $-m, -(m-1), \dots, -1, 0, 1, \dots, m-1, m$ . The standard deviation of these number is  $\sqrt{\frac{1}{3}m(m+1)}$ . For this to be an integer, we must have  $\frac{1}{3}m(m+1) = k^2$  for some integer  $k$ .  $m^2 = m = 3k^2$ ;  $n^2 = (2m+1)^2 = 12k^2 + 1$ . The smallest positive solution of the Pell equation  $n^2 - 12k^2 = 1$  being  $(7, 2)$ , the solutions of this equations are given by  $(n_i, k_i)$ , where

$$\begin{aligned} n_{i+1} &= 7n_i + 24k_i, \\ k_{i+1} &= 2n_i + 7k_i, \quad n_0 = 1, k_0 = 0. \end{aligned}$$

The beginning values of  $n$  and  $k$  are

$i$	1	2	3	4	5	6	7	8	...
$n_i$	7	97	1351	18817	262087	3650401	50843527	708158977	...
$k_i$	2	28	390	5432	75658	1053780	14677262	204427888	...

3. Find all Pythagorean triangles the lengths of whose two shorter sides differ by 1.

Let  $x$  and  $x + 1$  be the two shorter sides of a Pythagorean triangle, with hypotenuse  $y$ . Then  $y^2 = x^2 + (x + 1)^2 = 2x^2 + 2x + 1$ . From this,  $2y^2 = (2x + 1)^2 + 1$ . The equation With  $z = 2x + 1$ , this reduces to the Pell equation  $z^2 - 2y^2 = -1$ , which we know has solutions, with the of this equations are  $(z_n, y_n)$  given recursively by smallest positive one  $(1, 1)$ , and the equation  $z^2 - 2y^2 = 1$  has smallest positive solution  $(3, 2)$ . It follows that the solutions are given recursively by

$$\begin{aligned} z_{n+1} &= 3z_n + 4y_n, \\ y_{n+1} &= 2z_n + 3y_n, \quad z_0 = 1, y_0 = 1. \end{aligned}$$

If we write  $z_n = 2x_n + 1$ , these become

$$\begin{aligned} x_{n+1} &= 3x_n + 2y_n + 1, \\ y_{n+1} &= 4x_n + 3y_n + 2, \quad x_0 = 0, y_0 = 1. \end{aligned}$$

The beginning values of  $x_n$  and  $y_n$  are as follows.

$n$	1	2	3	4	5	6	7	8	9	10	...
$x_n$	3	20	119	696	4059	23660	137903	803760	4684659	27304196	...
$y_n$	5	29	169	985	5741	33461	195025	1136689	6625109	38613965	...

4. Find eleven consecutive positive integers, the sum of whose squares is the square of an integer.

*Answer:*

$$\begin{aligned} 18^2 + 19^2 + \cdots + 28^2 &= 77^2, \\ 38^2 + 39^2 + \cdots + 48^2 &= 143^2, \\ 456^2 + 457^2 + \cdots + 466^2 &= 1529^2, \\ 854^2 + 855^2 + \cdots + 864^2 &= 2849^2, \\ 9192^2 + 9193^2 + \cdots + 9202^2 &= 30503^2, \\ 17132^2 + 17133^2 + \cdots + 17142^2 &= 56837^2, \\ &\vdots \end{aligned}$$

## Chapter 13

# Elliptic Curves

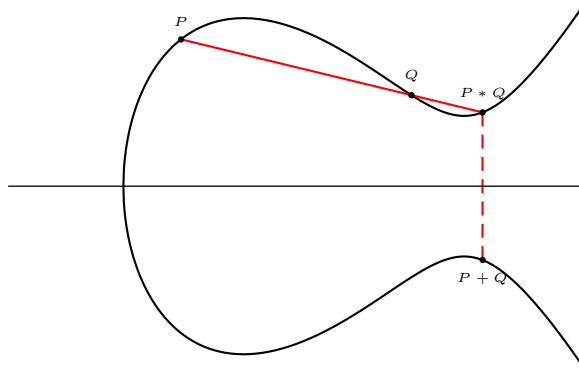
### 13.1 Group law on $y^2 = x^3 + ax^2 + bx + c$

Consider an elliptic curve

$$(\mathcal{E}) \quad y^2 = f(x) := x^3 + ax^2 + bx + c.$$

We shall write a point  $P$  on  $(E)$  in the form  $P = (x[P], y[P])$ , and put the identity at a point of infinity, so that

$$y[-P] = -y[P].$$



Consider a line of slope  $m$  passing through  $P$ . It has equation  $y - y[P] = m(x - x[P])$ . It intersects the elliptic curve  $(E)$  at points whose  $x$ -coordinates are the roots of the equation

$$(mx + (y[P] - mx[P]))^2 = x^3 + ax^2 + bx + c,$$

or equivalently,

$$x^3 - (m^2 - a)x^2 - (2m(y[P] - mx[P]) - b)x + c - (y[P] - mx[P])^2 = 0.$$

Since the sum of the three roots of the cubic is  $m^2 - a$ , we make the following conclusions.

(1) If the line is the tangent at  $P$ , then

(i)  $m = \frac{f'(x[P])}{2y[P]},$

(ii) the third intersection has  $x$ -coordinate

$$\begin{aligned} m^2 - a - 2x[P] &= \frac{f'(x[P])^2}{4y[P]^2} - a - 2x[P] \\ &= \frac{x[P]^4 - 2bx[P]^2 - 8cx[P] + (b^2 - 4ac)}{4y[P]^2} \\ &= \frac{x[P]^4 - 2bx[P]^2 - 8cx[P] + (b^2 - 4ac)}{4(x[P]^3 + ax[P]^2 + bx[P] + c)}. \end{aligned}$$

The  $y$ -coordinate can be computed from the equation of the line.

$$x[2P] = \frac{x[P]^4 - 2bx[P]^2 - 8cx[P] + (b^2 - 4ac)}{4(x[P]^3 + ax[P]^2 + bx[P] + c)}.$$

(2) If the line joins two points  $P_1$  and  $P_2$  on  $(E)$ , then

(i)  $m = \frac{y[P_1] - y[P_2]}{x[P_1] - x[P_2]},$

(ii) the third intersection has  $x$ -coordinate

$$\begin{aligned} &m^2 - a - x[P_1] - x[P_2] \\ &= \left( \frac{y[P_1] - y[P_2]}{x[P_1] - x[P_2]} \right)^2 - a - (x[P_1] + x[P_2]) \\ &= \frac{x[P_1]x[P_2](x[P_1] + x[P_2] + 2a) + b(x[P_1] + x[P_2]) + 2c - 2y[P_1]y[P_2]}{(x[P_1] - x[P_2])^2}. \end{aligned}$$

The  $y$ -coordinate can be computed from the equation of the line.

### 13.2 The discriminant

The discriminant of the cubic  $f(x) := x^3 + ax^2 + bx + c$  is the number

$$D := -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

**Theorem 13.1 (Nagell-Lutz).** *Let  $P = (x, y)$  be a finite order point of  $(\mathcal{E}) : y^2 = x^3 + ax^2 + bx + c$ . Then either  $y = 0$  (in which case  $P$  has order 2) or  $y^2 | D$ .*

**Theorem 13.2 (Mazur).** *The torsion group of the rational points of an elliptic curve over  $\mathbb{Q}$  is one of the following 15 groups:*

- (i)  $\mathbb{Z}_n$  with  $n = 1, 2, 3, \dots, 9, 10, 12$ ;
- (ii)  $\mathbb{Z}_{2n} \oplus \mathbb{Z}_2$  with  $n = 1, 2, 3, 4$ .

**Example 13.1.**

Elliptic Curve	Torsion group	Discriminant
$y^2 = x^3 + 2$	0	$-2^2 \cdot 3^3$
$y^2 = x^3 + x$	$\mathbf{Z}_2$	$-2^2$
$y^2 = x^3 + 4$	$\mathbf{Z}_3$	$-2^4 \cdot 3^3$
$y^2 = x^3 + 4x$	$\mathbf{Z}_4$	$-2^8$



## Chapter 14

# Heron triangles and Elliptic Curves

### 14.1 The elliptic curve $y^2 = (x - k)^2 - 4kx^3$

A triangle is determined, up to similarity, by a set of three positive real numbers  $\{t_1, t_2, t_3\}$  satisfying the relation

$$t_1t_2 + t_2t_3 + t_3t_1 = 1. \quad (14.1)$$

Such are indeed the tangents of the half - angles of the triangle. If the triangle is scaled to have unit semiperimeter, the lengths of the sides are

$$t_1(t_2 + t_3), \quad t_2(t_3 + t_1), \quad \text{and} \quad t_3(t_1 + t_2),$$

and the area is  $k = t_1t_2t_3$ . From the inequality of arithmetic and geometric means, it is easy to see that  $k^2 \leq \frac{1}{27}$ , with equality precisely in the case of an equilateral triangle. We study triangles with rational sides and rational areas. It is clear that for such triangles, the parameters  $t_1$ ,  $t_2$ , and  $t_3$  are all rational. Since such triangles cannot be equilateral, we shall assume  $k^2 < \frac{1}{27}$ . Elimination of  $t_3$  leads to

$$t_1^2t_2^2 - (t_1 - k)t_2 + kt_1 = 0.$$

A given rational number  $t_1$  determines a rational number  $t_2$ , and consequently a triangle with rational sides and rational area, if and only if  $(t_1 - k)^2 - 4kt_1^3$  is a rational square. A rational point  $(x, y)$  on the elliptic curve

$$\mathcal{E}_k : \quad y^2 = (x - k)^2 - 4kx^3,$$

therefore, determines rational numbers

$$t_1 = x, \quad t_2 = \frac{x + y - k}{2x^2}, \quad t_3 = \frac{x - y - k}{2x^2}. \quad (14.2)$$

These parameters in turn define a genuine triangle provided  $x > k$ , (see Lemma 2 below), the sides of the triangles being

$$\begin{aligned} a &= t_1(t_2 + t_3) = \frac{x - k}{x}, \\ b &= t_2(t_3 + t_1) = \frac{x + y + k}{2x}, \\ c &= t_3(t_1 + t_2) = \frac{x - y + k}{2x}. \end{aligned}$$

Given a triangle with unit semiperimeter and rational area  $k$ , we shall show that the associated elliptic curves  $\mathcal{E}_k$  has positive rank, provided that the triangle is non-isosceles. This leads to the following theorem on the existence of arbitrary number of Heron triangles equal in perimeter and in area.

**Theorem 14.1.** *Given a non-isosceles rational triangle  $T$  (of semiperimeter 1) and a positive integer  $N$ , there are an integer  $s$  and  $N$  noncongruent Heron triangles all having the same area and perimeter as  $sT$ .*

The qualification of non-isosceles triangle is essential. An example is provided by the case of the isosceles with sides (5,5,6), with  $t_1 = t_2 = \frac{1}{2}$ , and  $t_3 = \frac{3}{4}$ , and  $k = t_1 t_2 t_3 = \frac{3}{16}$ . The elliptic curve  $\mathcal{E}_k$  has rank 0, (See Proposition 10), showing that there are no other triangles of unit semiperimeter with the same value of  $k$ . However, such an isosceles triangle has equal perimeter and equal area as another isosceles triangle, then the elliptic curve has positive rank, and the statement of the theorem remains valid.

Guy [??, D16] reports that the problem of finding as many different triples of positive integers as possible with the same sum and the same product has been solved by A. Schinzel, that there are arbitrarily many. Theorem 1 offers a solution to the same problem: an arbitrary number of such triples, with the additional property that the sum and the product multiply to a square, can be constructed from any triple of distinct positive integers  $x, y, z$  with the same property, *i.e.*,  $xyz(x + y + z) = A^2$  for an integer  $A$ . Any such triple defines a Heron triangle with sides  $x + y, y + z, z + x$ , and area  $A$ .

Let  $k$  be a rational number  $< \frac{1}{3\sqrt{3}}$ . The cubic polynomial

$$f_k(x) := (x - k)^2 - 4kx^3 \tag{14.3}$$

has three distinct real roots separated by  $k$  and  $3k$ , since

$$\begin{aligned} f(-\infty) &= +\infty, \\ f(k) &= -4k^4 < 0, \\ f(3k) &= 4k^2(1 - 27k^2) > 0, \\ f(+\infty) &= -\infty. \end{aligned}$$

This means that the elliptic curve  $\mathcal{E}_k$  has two components, one of which is compact. A point  $(x, y)$  on  $\mathcal{E}_k$  lies in the compact component if and only if  $x > k$ . By Lemma 2 below, a point on  $\mathcal{E}_k$  corresponds to a genuine triangle if and only if its lies in the compact component.

**Lemma 14.2.** *A point  $(x, y)$  on the elliptic curve  $\mathcal{E}_k$  defines a genuine triangle if and only if  $x > k$ .*

*Proof.* From (14.2),  $t_2 + t_3 = \frac{x-k}{x^2}$  and  $t_2t_3 = \frac{y^2}{4x^4}$ . It is clear that  $t_1, t_2, t_3$  are all positive (and defines a genuine triangle) if and only if  $x > k$ .  $\square$

The addition law of  $\mathcal{E}_k$  is given by

$$x(P + Q) = \frac{1}{4k}(1 - \lambda^2) - x(P) - x(Q),$$

where

$$\lambda = \begin{cases} \frac{y(P)-y(Q)}{x(P)-x(Q)}, & \text{if } P \neq Q, \\ \frac{x(P)-k-6k \cdot x(P)^2}{y(P)}, & \text{if } P = Q. \end{cases}$$

**Lemma 14.3.** *Let  $P$  be a point on the compact component of  $\mathcal{E}_K$ . The six points  $\pm P, \pm P \pm I$  all represent the same (similarity class of) rational triangles.*

*Proof.* Write  $P = (t_1, t_1^2(t_2 - t_3))$ . Then, for  $\epsilon = \pm 1$ ,

$$\begin{aligned} \epsilon(P + I) &= (t_2, \epsilon t_2^2(t_3 - t_1)), \\ \epsilon(P - I) &= (t_3, \epsilon t_3^2(t_1 - t_2)). \end{aligned}$$

Let  $P$  and  $Q$  be two distinct points on  $\mathcal{E}_k$ , one on each of the two components. By the convexity of the compact component, it is clear that

the sum  $P+Q$  lies in the compact component. Now, if  $P$  is a point in the compact component, then  $2P$  must be in the noncompact one. It follows by induction that all odd multiples of  $P$  are in the compact component, and hence define genuine rational triangles.

**Example 14.1.** For  $k = \frac{1}{6}$ , the cubic polynomial  $f_k(x) = \frac{1}{36}(1 - 12x + 36x^2 - 24x^3)$  is irreducible.

**Example 14.2.** For  $k = \frac{168}{1331} = \frac{2^3 \cdot 3 \cdot 7}{11^3}$ , the cubic polynomial

$$f_k(x) = -4k\left(x - \frac{56}{33}\right)\left(x^2 - \frac{699}{2464}x + \frac{9}{484}\right).$$

The rational root  $\frac{56}{33}$  corresponds to the isosceles Heron triangle (65, 65, 112). On the same curve, there are rational points with  $x = \frac{2}{11}, \frac{8}{11}, \frac{21}{22}$ , corresponding to the Heron triangle (37, 100, 105), also of perimeter 242 and area 1848.

**Example 14.3.** For  $k = \frac{60}{343}$ , the cubic polynomial  $f_k(x)$  has three rational roots  $\frac{15}{112} < \frac{12}{35} < \frac{20}{21}$ . The larger two correspond respectively to the isosceles triangles (24, 37, 37) and (29, 29, 40), both with perimeters 98 and area 420. On  $\mathcal{E}_k$  lie also the rational points with  $x = \frac{5}{14}, \frac{4}{7}, \frac{6}{7}$ , corresponding to the Heron triangle (25, 34, 39), with the same perimeter and area.

#### 14.1.1 Proof of Theorem 14.1

A non-isosceles triangle with semiperimeter 1 and area  $k$  corresponds to a point  $P$  in the component of the elliptic curve  $\mathcal{E}_k$ . Such a point cannot have finite order, and so generates an infinite cyclic subgroup of  $\mathcal{E}_k$ . The points  $mP$  lies in the compact component precisely when  $m$  is odd. For any given integer  $N$ , the points  $(2m-1)P$ ,  $1 \leq m \leq N$ , all lie in the compact component, and therefore represent rational triangles  $T_m$ , each of semiperimeter 1 and area  $k$ . Let  $s$  be the least common multiple of the denominators of the lengths of sides of these  $N$  triangles. Magnifying each of them by the factor  $s$ , we obtain a sequence of  $N$  Heron triangles, all with semiperimeter  $s$ , and area  $ks^2$ .  $\square$

**Example 14.4.** The right triangle (3,4,5) corresponds to the point  $P(1, \frac{1}{6})$  on the curve  $\mathcal{E}_{1/6}$ . The primitive Heron triangles corresponding the points  $P, 3P, 5P, 7P$ , and  $9P$ , with their semiperimeters and areas, are as follows.

(3, 4, 5; 6, 6),  
 (287, 468, 505; 630, 66150),  
 (3959527, 3997940, 5810001; 6883734, 7897632297126),  
 (3606573416251, 5935203156525, 6344028032612; 7942902302694,  
 10514949498356941266609606),  
 (480700822846118327460, 630296830413008002763, 795751643958885119197;  
 953374648609005724710, 151487203435057523536941712814925384097350).

The LCM of the semiperimeters being

$$s = 1447986121797526457728510272387457724310,$$

magnifying these triangles by appropriate factors, we obtain five Heron triangles, all with semiperimeter  $s$  and area

$$\Delta = 349443968153040187579733428603820320155254000034420331290213618794580660829350.$$

The following example shows that the hypothesis of non-isoscelesity is essential.

*Remark.* Let  $k = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{3}{4} = \frac{3}{16}$ . The elliptic curve is cyclic of order 6. In particular, it has rank 0.

This value of  $k$  arises from the isosceles triangle (5, 5, 6). By Proposition 7, there is no other (noncongruent) triangle of unit semiperimeter and the same area. On the other hand, Example 1 shows that for the isosceles triangle (65, 65, 126), the associated elliptic curve has positive rank.



# Supplements and Corrections

## 5.1

The partial solution of the exercise should be replaced by the following.

Let  $u = s - a$  and  $v = s - b$ . Since  $r = s - c$  for a right triangle, we have  $(u+r)^2 + (v+r)^2 = (u+v)^2$ . This can be rearranged as  $(u-r)(v-r) = 2r^2$ . Each factorization of  $2r^2$  into the product of two numbers gives  $u$  and  $v$  up to an interchanges, and one Pythagorean triangle of inradius  $r$ . There are  $\frac{1}{2}d(2r^2)$  such pairs, where  $d$  is the number-of-divisors function.

## 5.5

Proposition 5.2 (3) should be replaced by the following.

(3) *For Pythagorean triangles of inradius  $r$ , there are exactly  $\frac{1}{2}d(2r^2)$  of such, where  $d$  is the number-of-divisors function.*

The proof for (3) should be replaced by the following.

If  $k$  is a divisor of  $2r^2$  greater than  $\sqrt{2}r$ , then  $u = r + k$  and  $v = r + \frac{2r^2}{k}$  give a Pythagorean triangle  $(r + v, r + u, u + v)$  with inradius  $r$ .

## 5.6 Enumeration of Pythagorean triangles according to inradii

According to (the supplement of) §5.1, we can make a complete list of Pythagorean triples arranged in ascending order of the inradius. For each positive integer  $r$ ,

- (i) list the divisors of  $2r^2$  in ascending order up to  $\sqrt{2}r$ ,
- (ii) for each factor  $k$ , set

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

See [10].

## 6.1

**Lemma 14.4.** *Let  $p$  be an odd prime. The residue  $-1$  is a square modulo  $p$  if and only if  $p \equiv 1 \pmod{4}$ .*

*Proof.* ( $\Leftarrow$ ) If  $p = 4k + 1$ , it follows from Wilson's theorem that

$$\begin{aligned} ((2k)!)^2 &\equiv (2k)! \cdot (p - 2k) \cdots (p - 1) \\ &= (2k)! \cdot (2k + 1) \cdots (p - 1) \\ &= (p - 1)! \equiv -1 \pmod{p}. \end{aligned}$$

( $\Rightarrow$ ) If  $x^2 \equiv -1 \pmod{p}$ , then

$$(-1)^{(p-1)/2} \equiv (x^2)^{(p-1)/2} = x^{p-1} \equiv 1 \pmod{p}$$

by Fermat's little theorem. It follows that  $\frac{p-1}{2}$  is an even integer, and  $p \equiv 1 \pmod{4}$ .  $\square$

In the proof of Theorem 6.1, replace each occurrence of  $x_1$  by  $u$  and  $y_1$  by  $v$ . The first part of the proof is rewritten with minor changes as follows.

Since  $p \equiv 1 \pmod{4}$ , the equation  $x^2 + y^2 = mp$  is solvable in integers for some  $m$ . We want to show that the *smallest* possible value of  $m$  is 1. Note that we may choose  $|x|, |y| < \frac{p}{2}$  so that  $m < \frac{p}{2}$ . If  $m \neq 1$ , it cannot divide *both* of  $x$  and  $y$ , for otherwise  $m^2 | x^2 + y^2 = mp$  and  $m | p$ , contrary to  $m < \frac{p}{2}$ . Now choose integers  $u$  and  $v$  in the range  $-\frac{m}{2} < u, v < \frac{m}{2}$  such that  $u \equiv x$  and  $v \equiv y \pmod{m}$ . Note that  $u$  and  $v$  cannot be both zero, and

$$0 < u^2 + v^2 \leq \frac{m^2}{2}.$$

It follows that  $u^2 + v^2 = m'm$  for some  $m' \leq \frac{m}{2} < m$ . Now,

$$m^2 m' p = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2, \quad (14.4)$$

Note that

$$\begin{aligned} xu + yv &\equiv x^2 + y^2 \equiv 0 \pmod{m}, \\ xv - yu &\equiv xy - yx \equiv 0 \pmod{m}. \end{aligned}$$

Therefore,  $X := \frac{xu+yv}{m}$  and  $Y := \frac{xv-yu}{m}$  are integers. From (14.4) it follows that

$$X^2 + Y^2 = m'p$$

with  $m' < m$ . By *descent*, we finally reach an equation  $x^2 + y^2 = p$ .  $\square$

Now, we summarize this descent step as follows.

Let  $q$  be the square root of  $-1 \pmod{p}$ , chosen in the range  $0 < q < \frac{p}{2}$ , and  $q^2 + 1 = mp$ . Let  $u$  and  $v$  be chosen in the range  $-\frac{p}{2} < u < \frac{p}{2}$  satisfying  $u \equiv q \pmod{p}$  and  $v = 1$ .

Let  $x_1 = q, y_1 = 1, m_1 = m, u_1 = u,$  and  $v_1 = 1$ .

Define  $(x_n, y_n, m_n, u_n, v_n)$  inductively as follows. If  $m_n = 1$ , then  $x_n^2 + y_n^2 = p$ . If  $m_n > 1$ , define

- (i)  $x_{n+1} = \frac{x_n u_n + y_n v_n}{m_n}$  and  $y_{n+1} = \frac{x_n v_n - y_n u_n}{m_n}$ ;
- (ii)  $m_{n+1} = \frac{x_{n+1}^2 + y_{n+1}^2}{p}$ ;
- (iii)  $u_{n+1}, v_{n+1}$  in the interval  $(-\frac{m_{n+1}}{2}, \frac{m_{n+1}}{2})$  such that  $u_{n+1} \equiv x_{n+1} \pmod{m_{n+1}}$  and  $v_{n+1} \equiv y_{n+1} \pmod{m_{n+1}}$ .

**Example 14.5.** For  $p = 3637$ , we have  $q = 1027$  and  $p = 39^2 + 46^2$  from the following table.

$n$	$x_n$	$y_n$	$m_n$	$u_n$	$v_n$
1	1027	1	290	-133	1
2	-471	4	61	17	4
3	-131	-32	5	-1	-2
4	39	46	1		

## Chapter 8

Page 401: **3.** The product of two quadratic residues mod  $n$  is not necessarily a quadratic residue mod  $n$ . For example, in  $\mathbb{Z}_{12}^\bullet = \{1, 5, 7, 11\}$ , only 1 is a quadratic residue; 5, 7, and  $11 \equiv 5 \cdot 7$  are all quadratic non-residues.

14.1.2 Theorem 11.4

Note the *symmetry* within a period of the continued fraction expansion of  $\sqrt{d}$ . We illustrate this with two examples.

(a). The continued fraction of  $\sqrt{94}$ . We shall compute that of  $9 + \sqrt{94}$ , which is purely periodic, since the quadratic irrationality  $9 + \sqrt{94}$  is reduced:

$k$	$\frac{1}{\zeta_{k-1} - q_{k-1}}$	$=$	$\zeta_k$	$=$	$q_k + (\zeta_k - q_k)$
0			$9 + \sqrt{94}$	$=$	$18 + (-9 + \sqrt{94})$
1	$\frac{1}{-9 + \sqrt{94}}$	$=$	$\frac{9 + \sqrt{94}}{13}$	$=$	$1 + \frac{-4 + \sqrt{94}}{13}$
2	$\frac{13}{-4 + \sqrt{94}}$	$=$	$\frac{4 + \sqrt{94}}{6}$	$=$	$2 + \frac{-8 + \sqrt{94}}{6}$
3	$\frac{6}{-8 + \sqrt{94}}$	$=$	$\frac{8 + \sqrt{94}}{5}$	$=$	$3 + \frac{-7 + \sqrt{94}}{5}$
4	$\frac{5}{-7 + \sqrt{94}}$	$=$	$\frac{7 + \sqrt{94}}{9}$	$=$	$1 + \frac{-2 + \sqrt{94}}{9}$
5	$\frac{9}{-2 + \sqrt{94}}$	$=$	$\frac{2 + \sqrt{94}}{10}$	$=$	$1 + \frac{-8 + \sqrt{94}}{10}$
6	$\frac{10}{-8 + \sqrt{94}}$	$=$	$\frac{8 + \sqrt{94}}{3}$	$=$	$5 + \frac{-7 + \sqrt{94}}{3}$
7	$\frac{3}{-7 + \sqrt{94}}$	$=$	$\frac{7 + \sqrt{94}}{15}$	$=$	$1 + \frac{-8 + \sqrt{94}}{15}$
8	$\frac{15}{-8 + \sqrt{94}}$	$=$	$\frac{8 + \sqrt{94}}{2}$	$=$	$8 + \frac{-8 + \sqrt{94}}{2}$
9	$\frac{2}{-8 + \sqrt{94}}$	$=$	$\frac{8 + \sqrt{94}}{15}$	$=$	$1 + \frac{-7 + \sqrt{94}}{15}$

It is here where symmetry begins when in  $\zeta_9 = q_9 + \frac{1}{\zeta_{10}}$ , we have  $\frac{1}{\zeta_{10}} = -\overline{\zeta_9}$ . This is because the preceding line

$$\zeta_8 = q_8 + \frac{1}{\zeta_9}$$

can be conjugated to give

$$\overline{\zeta_8} = q_8 + \frac{1}{\overline{\zeta_9}} = q_8 - \zeta_{10}.$$

In other words,

$$\zeta_{10} = q_8 + (-\overline{\zeta_8}).$$

Note that since  $\zeta_8$  is reduced, this last term is between 0 and  $-1$ . This means  $q_9 = q_8$  and  $\frac{1}{\zeta_{10}} = -\overline{\zeta_8}$ . By iteration, we obtain the sequence  $q_8, q_7, \dots, q_1$ , and

$$\begin{aligned} 9 + \sqrt{94} &= [18, 1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1]; \\ \sqrt{94} &= [9, 1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18]. \end{aligned}$$

In this case, the period has *even* length.

(b) Another kind of symmetry occurs in the expansions of, say,  $\sqrt{97}$ . Again, we compute the purely periodic expansion of  $9 + \sqrt{97}$ :

$$\begin{array}{rclclcl}
 k & \frac{1}{\zeta_{k-1} - q_{k-1}} & = & \zeta_k & = & q_k + (\zeta_k - q_k) \\
 0 & & & 9 + \sqrt{97} & = & 18 + (-9 + \sqrt{97}) \\
 1 & \frac{1}{-9 + \sqrt{97}} & = & \frac{9 + \sqrt{97}}{16} & = & 1 + \frac{-7 + \sqrt{97}}{16} \\
 2 & \frac{16}{-7 + \sqrt{97}} & = & \frac{7 + \sqrt{97}}{3} & = & 5 + \frac{-8 + \sqrt{97}}{3} \\
 3 & \frac{3}{-8 + \sqrt{97}} & = & \frac{8 + \sqrt{97}}{11} & = & 1 + \frac{-3 + \sqrt{97}}{11} \\
 4 & \frac{11}{-3 + \sqrt{97}} & = & \frac{3 + \sqrt{97}}{8} & = & 1 + \frac{-5 + \sqrt{97}}{8} \\
 5 & \frac{8}{-5 + \sqrt{97}} & = & \frac{5 + \sqrt{97}}{9} & = & 1 + \frac{-4 + \sqrt{97}}{9} \\
 6 & \frac{9}{-4 + \sqrt{97}} & = & \frac{4 + \sqrt{97}}{9} & & 
 \end{array}$$

Here, we have  $\frac{1}{\zeta_6} = -\overline{\zeta_6}$ . In fact,

$$\begin{aligned}
 \zeta_5 &= q_5 + \frac{1}{\zeta_6} = q_5 - \overline{\zeta_6}, \\
 \overline{\zeta_6} &= q_5 - \zeta_5, \\
 \zeta_6 &= q_5 + (-\zeta_5).
 \end{aligned}$$

This means  $q_7 = q_5$  and  $\frac{1}{\zeta_8} = -\overline{\zeta_6}$ . Symmetry emerges by iteration, and we have

$$\begin{aligned}
 9 + \sqrt{97} &= [18, 1, 5, 1, 1, 1, 1, 1, 1, 5, 1]; \\
 \sqrt{97} &= [9, 1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18].
 \end{aligned}$$

In this case, the period has *odd* length.

## Chapter 12

### Approximations to Irrational Numbers

**Theorem 14.5.** *Let  $\zeta$  be an irrational number. If a rational approximation  $\frac{P}{Q}$ ,  $Q \geq 1$ , satisfies*

$$\left| \zeta - \frac{P}{Q} \right| < \frac{1}{2Q^2},$$

*then  $\frac{P}{Q}$  is one of the convergents of the continued fraction expansion of  $\zeta$ .*

*Proof.* (1)  $|Q_n\zeta - P_n| < \frac{1}{Q_{n+1}}$ .

$$\begin{aligned} \left| \zeta - \frac{P_n}{Q_n} \right| &= \left| \frac{P_{n-1} + P_n\xi_{n+1}}{Q_{n-1} + Q_n\xi_{n+1}} - \frac{P_n}{Q_n} \right| \\ &\vdots \\ &= \frac{1}{Q_n(Q_{n-1} + Q_n\xi_{n+1})} \\ &< \frac{1}{Q_n(Q_{n-1} + Q_n a_{n+1})} \\ &= \frac{1}{Q_n Q_{n+1}}. \end{aligned}$$

The inequality follows by multiplying by  $Q_n$ .

(2) If  $\frac{P}{Q}$ ,  $Q > 0$ , satisfies  $|Q\zeta - P| < |Q_n\zeta - P_n|$  for some  $n \geq 1$ . Then,  $Q \geq Q_{n+1}$ .

Suppose  $|Q\zeta - P| < |Q_n\zeta - P_n|$  for  $Q < Q_{n+1}$ . We can find integers  $x$  and  $y$  satisfying

$$\begin{aligned} xP_n + yP_{n+1} &= P, \\ xQ_n + yQ_{n+1} &= Q. \end{aligned}$$

Actually,  $x = (-1)^n(PQ_{n+1} - QP_{n+1})$  and  $y = (-1)^n(P_nQ - Q_nP)$ . Since  $\frac{P}{Q}$  is different from  $\frac{P_n}{Q_n}$  and  $\frac{P_{n+1}}{Q_{n+1}}$ ,  $x$  and  $y$  are nonzero.

First note that  $x$  and  $y$  must be nonzero. If any of  $x$ ,  $y$  is zero, then  $\frac{P}{Q}$  is one of  $\frac{P_n}{Q_n}$  and  $\frac{P_{n+1}}{Q_{n+1}}$ . Indeed,  $x$  and  $y$  have opposite signs.

If  $y < 0$ , then  $xQ_n = Q - yQ_{n+1} > 0$ , and  $x > 0$ .

If  $y > 0$ , then  $Q < Q_{n+1}$  implies  $Q < yQ_{n+1}$  and  $x_nQ_n$  must be negative, and  $x < 0$ .

These justify that claim that  $x$  and  $y$  have opposite signs. Consequently,  $x(Q_n\zeta - P_n)$  and  $y(Q_{n+1}\zeta - P_{n+1})$  have the same sign, and

$$\begin{aligned} |Q\zeta - P| &= |x(Q_n\zeta - P_n) + y(Q_{n+1}\zeta - P_{n+1})| \\ &= |x(Q_n\zeta - P_n)| + |y(Q_{n+1}\zeta - P_{n+1})| \\ &> |Q_n\zeta - P_n|, \end{aligned}$$

a contradiction.

(3) Suppose  $\frac{P}{Q}$  is not a convergent of  $\zeta$ . Then  $Q_n < Q < Q_{n+1}$  for some  $n$ . But  $|Q\zeta - P| < |Q_n\zeta - P_n|$  is impossible. Therefore,

$$|Q_n\zeta - P_n| \leq |Q\zeta - P| < \frac{1}{2Q}.$$

Now, using the fact that  $\frac{P}{Q} \neq \frac{P_n}{Q_n}$  and that  $QP_n - PQ_n$  is an integer, we have

$$\left| \frac{P_n}{Q_n} - \frac{P}{Q} \right| = \frac{|QP_n - PQ_n|}{QQ_n} \geq \frac{1}{QQ_n},$$

and

$$\left| \frac{P_n}{Q_n} - \frac{P}{Q} \right| \leq \left| \zeta - \frac{P_n}{Q_n} \right| + \left| \zeta - \frac{P}{Q} \right| < \frac{1}{2QQ_n} + \frac{1}{2Q^2}.$$

By comparison,  $Q < Q_n$ , an impossibility.  $\square$

### Theorem 12.2

Replaced by the following with minor change of notations.

**Theorem 14.6.** *Let  $s$  be an integer satisfying  $|s| < \sqrt{d}$ . If  $(x, y) = (P, Q)$  is a positive solution of the equation*

$$x^2 - dy^2 = s$$

*then  $\frac{P}{Q}$  is a convergent of the continued fraction expansion of  $\sqrt{d}$ .*

*Proof.* Case 1:  $s > 0$ . Writing  $s = (P + Q\sqrt{d})(P - Q\sqrt{d})$ , we have

$$\begin{aligned} 0 < P - Q\sqrt{d} &= \frac{s}{P + Q\sqrt{d}} < \frac{\sqrt{d}}{P + Q\sqrt{d}} \\ &= \frac{1}{Q(1 + \frac{P}{Q\sqrt{d}})} < \frac{1}{2Q}. \end{aligned}$$

From this,

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

and  $\frac{P}{Q}$  is a convergent of the continued fraction expansion of  $\xi$ .

Case 2:  $s < 0$ . Rewriting the equation as  $\frac{-s}{d} = (Q + \frac{P}{\sqrt{d}})(Q - \frac{P}{\sqrt{d}})$ , we have

$$\begin{aligned} 0 < Q - \frac{P}{\sqrt{d}} &= \frac{\frac{-s}{d}}{Q + \frac{P}{\sqrt{d}}} < \frac{\frac{1}{\sqrt{d}}}{Q + \frac{P}{\sqrt{d}}} \\ &= \frac{1}{P + Q\sqrt{d}} = \frac{1}{P(1 + \frac{Q\sqrt{d}}{P})} < \frac{1}{2P}. \end{aligned}$$

Therefore,

$$\left| \frac{1}{\sqrt{d}} - \frac{Q}{P} \right| < \frac{1}{2P^2}$$

and  $\frac{Q}{P}$  is a convergent of  $\frac{1}{\sqrt{d}}$ , and  $\frac{P}{Q}$  one of  $\sqrt{d}$ .  $\square$

### Proof of Theorem 12.3

For an arbitrary (but fixed) integer  $s$ , consider the equation  $E(d, s)$ , with solution set  $\mathcal{S}_d(s)$  as a subset of  $\mathbb{Z}[\sqrt{d}]$ . We define a relation  $\approx$  in  $\mathcal{S}_d(s)$  by

$$\alpha \approx \beta \text{ if and only if } \alpha\beta^{-1} \in \mathbb{Z}[\sqrt{d}].$$

This clearly is an equivalence relation. The solutions of  $E(d, s)$  therefore are partitioned into disjoint classes.

In generally, the class of  $\alpha$  and that of  $\bar{\alpha}$  are disjoint. But sometimes, they may coincide. In that case, we say that the class is ambiguous.

Clearly, for  $s = \pm 1$ , there is only one class, and the class is ambiguous.

We shall therefore assume  $s \neq \pm 1$ . Note that each class of  $\mathcal{S}_d(s)$  is infinite. In fact, if  $\epsilon := a + b\sqrt{d}$  is the fundamental solution of  $E(d)$ , the class of  $\alpha$  contains  $\alpha \cdot \epsilon^n$ ,  $n \in \mathbb{Z}$ . In each class, we choose the solution with least possible *non-negative* second component. This uniquely determines the first component, except in the ambiguous case. In this case, we stipulate that the first component be non-negative. In this way, in each class, we single out a *fundamental solution*.

#### Theorem 12.3A.

Let  $s > 0$ . If  $u + v\sqrt{d}$  is the fundamental solution of  $E(d, s)$ , then

$$0 \leq v \leq \frac{b}{\sqrt{2(a+1)}} \cdot \sqrt{s},$$

$$0 < |u| \leq \sqrt{\frac{1}{2}(a+1)s}.$$

*Proof.* We may assume  $u > 0$ . Consider

$$(u + v\sqrt{d})(a - b\sqrt{d}) = (au - dbv) + (av - bu)\sqrt{d}.$$

This clearly belongs to the same class of  $u + v\sqrt{d} \in \mathcal{S}_d(s)$ . Now, since

$$au - dbv = au - \sqrt{db^2 \cdot dv^2} = au - \sqrt{(a^2 - 1)(u^2 - s)} > 0,$$

we must have  $au - dbv \geq u$ . From this it follows that

$$(a - 1)^2 u^2 \geq d^2 b^2 v^2 = (a^2 - 1)(u^2 - s),$$

and

$$u^2 \leq \frac{1}{2}(a + 1)s.$$

This completes the proof.

**Theorem 12.3B.**

Let  $s > 0$ . If  $u + v\sqrt{d}$  is the fundamental solution of  $E(d, -s)$ , then

$$0 < \frac{b}{\sqrt{2(a-1)}} \cdot \sqrt{s},$$

$$0 \leq |u| \leq \sqrt{\frac{1}{2}(a-1)s}.$$

*Proof.* We may again suppose  $u \geq 0$ . Again,

$$(a - b\sqrt{d})(u + v\sqrt{d}) = (au - dbv) + (av - bu)\sqrt{d}$$

is in  $\mathfrak{S}_d(s)$ . Since

$$(av)^2 = a^2 \cdot v^2 = (db^2 + 1) \cdot \frac{1}{d}(u^2 + s) = (b^2 + \frac{1}{d})(u^2 + s) > (bu)^2,$$

it follows that  $av - bu > 0$ , and indeed  $av - bu \geq v$ . From this

$$dv^2(a - 1)^2 \geq db^2u^2,$$

$$(u^2 + s)(a - 1)^2 \geq (a^2 - 1)u^2,$$

$$u^2 \leq \frac{1}{2}(a - 1)s.$$

## Chapter 12. Sums of consecutive squares

### Sums of an odd number of consecutive squares

Suppose the sum of the squares of  $2k + 1$  consecutive *positive* integers is a square. If the integers are  $b, b \pm 1, \dots, b \pm k$ . We require

$$(2k + 1)b^2 + \frac{1}{3}k(k + 1)(2k + 1) = a^2$$

for an integer  $a$ . From this we obtain the equation

$$a^2 - (2k + 1)b^2 = \frac{1}{3}k(k + 1)(2k + 1). \quad (E_k)$$

### Exercise

1. Suppose  $2k + 1$  is a square. Show that  $(E_k)$  has solution only when  $k = 6m(m + \epsilon)$  for some integers  $m > 1$ , and  $\epsilon = \pm 1$ . In each case, the number of solutions is *finite*.

#### Number of solutions of $(E_k)$ when $2k + 1$ is a square

$2k + 1$	25	49	121	169	289	361	529	625	841	961	...
	0	1	1	2	7	3	5	3	3	10	...

2. Find the *unique* sequence of 49 (respectively 121) consecutive positive integers whose squares sum to a square.

*Answer:*  $25^2 + 26^2 + \dots + 73^2 = 357^2$ ;  $244^2 + 245^2 + \dots + 364^2 = 3366^2$ ;

*Remark:* The two sequences of 169 consecutive squares whose sums are squares are

$$\begin{aligned} 30^2 + 31^2 + \dots + 198^2 &= 1612^2; \\ 510^2 + 511^2 + \dots + 678^2 &= 7748^2. \end{aligned}$$

3. Suppose  $2k + 1$  is not a square. If  $k + 1$  is divisible  $9 = 3^2$  or by any prime of the form  $4k + 3 \geq 7$ , then the equation  $(E_k)$  has no solution.

4. Show that for the following values of  $k < 50$ , the equation  $(E_k)$  has no solution:

$$k = 6, 8, 10, 13, 17, 18, 20, 21, 22, 26, 27, 30, 32,$$

34, 35, 37, 40, 41, 42, 44, 45, 46, 48, ...

5. Suppose  $p = 2k + 1$  is a prime. If the Legendre symbol  $\left(\frac{-\frac{1}{3}k(k+1)}{p}\right) = -1$ , then the equation  $(E_k)$  has *no* solution.

6. Show that for the following values of  $k < 50$ , the equation  $(E_k)$  has no solution:

1, 2, 3, 8, 9, 14, 15, 20, 21, 26, 33, 39, 44.

We need only consider  $(E_k)$  for the following values of  $k$ :

5, 7, 11, 16, 19, 23, 25, 28, 29, 31, 36, 38, 43, 47, 49.

7. Use Theorem 12.3 to check that among these, only for  $k = 5, 11, 16, 23, 29$  are the equations  $(E_k)$  solvable.

8. From the data of Example 12.1, work out 5 sequences of 23 consecutive integers whose squares add up to a square in each case.

*Answer:*

$$\begin{aligned} 7^2 + 8^2 + \cdots + 29^2 &= 92^2; \\ 881^2 + 882^2 + \cdots + 903^2 &= 4278^2; \\ 42787^2 + 42788^2 + \cdots + 42809^2 &= 205252^2; \\ 2053401^2 + 2053402^2 + \cdots + 2053423^2 &= 9847818^2; \\ &\dots \end{aligned}$$

9. Consider the equation  $(E_{36}) : a^2 - 73b^2 = 12 \cdot 37 \cdot 73$ . Check by Theorem 10.6.3 that this equation does in fact have solutions  $(u, v) = (4088, 478), (23360, 2734)$ .

10. Make use of the fundamental solution of  $x^2 - 73y^2 = 1$ , namely,  $(a, b) = (2281249, 267000)$ , to obtain two sequences of solutions of  $(E_{73})$ :

*Answer:*

$$\begin{aligned} &(4088, 478), (18642443912, 2181933022), (85056113063608088, 9955065049008478), \dots \\ &(23360, 2734), (106578370640, 12474054766), (486263602888235360, 56912849921762734), \dots \end{aligned}$$

This means, for example, the sum of the squares of the 73 numbers with center 478 (respectively 2734) is equal to the square of 4088 (respectively 23360).

**Even number of consecutive squares**

Suppose the sum of the squares of the  $2k$  consecutive numbers

$$b - k + 1, b - k + 2, \dots, b, \dots, b + k - 1, b + k,$$

is equal to  $a^2$ . This means

$$(2a)^2 - 2k(2b + 1)^2 = \frac{2k}{3}(4k^2 - 1). \quad (E'_k)$$

Note that the numbers  $2k, 4k^2 - 1$  are relatively prime.

**Exercise**

1. Show that the equation  $(E'_k)$  has no solution if  $2k$  is a square.
2. Suppose  $2k$  is not a square. Show that if  $2k + 1$  is divisible by 9, or by any prime of the form  $4k + 1$ , then the equation  $(E'_k)$  has no solution.
3. Show that for  $k \leq 50$ , the equation  $(E'_k)$  has no solution for the following values of  $k$ :

$$k = 3, 4, 5, 9, 11, 13, 15, 17, 21, 23, 24, 27, 29, 31, 33, \\ 35, 38, 39, 40, 41, 45, 47, 49.$$

4. Let  $k$  be a prime. Show that the equation  $(E'_k)$  can be written as

$$(2b + 1)^2 - 2ky^2 = -\frac{4k^2 - 1}{3}.$$

By considering Legendre symbols, show that the equation  $(E'_k)$  has no solution for the following values of  $k \leq 50$ :

$$k = 5, 7, 17, 19, 29, 31, 41, 43.$$

5. By using Theorem 12.3, check that, excluding square values of  $2k < 100$ , the equation  $(E'_k)$  has solutions only for  $k = 1, 12, 37, 44$ .

The case  $2k = 2$  has been dealt with in §12.4, Example 3.

6. Show that  $(34, 0), (38, 3), (50, 7)$  are solutions of  $(E''_{12})$ . Construct from them three infinite sequences of expressions of the sum of 24 consecutive squares as a square.

*Answer:*

$$25^2 + 26^2 + \dots + 48^2 = 182^2; \\ 44^2 + 45^2 + \dots + 67^2 = 274^2;$$

$$76^2 + 77^2 + \cdots + 99^2 = 430^2.$$

7. Show that  $(185, 2)$ ,  $(2257, 261)$ , and  $(2849, 330)$  are solutions of  $(E'_{37})$ . Construct from them three infinite sequences of expressions of the sum of 74 consecutive squares as a square.

*Answer:*

$$\begin{aligned} 225^2 + 226^2 + \cdots + 298^2 &= 2257^2; \\ 294^2 + 295^2 + \cdots + 367^2 &= 2849^2; \\ 13096^2 + 13097^2 + \cdots + 13179^2 &= 763865^2. \end{aligned}$$

8. Show that  $(242, 4)$  and  $(2222, 235)$  are solutions of  $(E'_{44})$ . Construct from them two infinite sequences of expressions of the sum of 88 consecutive squares as a square.

*Answer:*

$$\begin{aligned} 192^2 + 193^2 + \cdots + 279^2 &= 2222^2; \\ 5925^2 + 5926^2 + \cdots + 6012^2 &= 55990^2. \end{aligned}$$

*Remark:* The equation  $(E'_{26}) : x^2 - 52y^2 = 18 \cdot 52 \cdot 53$  does indeed have two infinite sequences of solutions generated by the particular solutions  $(338, 36)$ ,  $(2002, 276)$ , and the fundamental solution  $(649, 90)$  of the Pell equation  $x^2 - 52y^2 = 1$ . None of these, however, leads to a solution of  $(E'_{26})$  since all the  $y$ 's are even.

### Lucas Problem

When does a square pyramid of cannon balls contain a number of cannon balls which is a perfect square? Lucas claimed that the only solutions of

$$1^2 + 2^2 + \cdots + n^2 = k^2$$

are  $(n, k) = (1, 1), (24, 70)$ . This was established by Watson in 1918.

### Pair of Heron triangles with equal areas and equal perimeters

To find a pair of Heron triangles with equal areas and equal perimeters, one of them similar to (5, 12, 13).

The given triangle (5, 12, 13) has  $s = 15$  and area 30. Scaled to unit semiperimeter, it has area  $k = \frac{2}{15}$ .

Consider a point on the elliptic curve

$$(E) : \quad y^2 = (x - k)^2 - 4kx^3.$$

The given triangle has one angle  $90^\circ$  and corresponding “half-tangent” equal to 1. This gives a point  $P$  on  $(E)$  with  $x = 1$ . In fact,  $P = (1, \frac{7}{15})$ .

If we have two points  $(x_1, y_1)$  and  $(x_2, y_2)$  on  $(E)$ , the line joining them has slope  $m = \frac{y_1 - y_2}{x_1 - x_2}$ . It intersects  $(E)$  again at a point  $(x_3, y_3)$ , with

$$x_1 + x_2 + x_3 = \frac{1 - m^2}{4k}.$$

Now, the tangent at  $P$  has slope  $m = \frac{1}{7}$ . Its tangent intersects  $(E)$  again at  $(x_3, y_3)$ , where

$$x_3 = \frac{1 - (\frac{1}{7})^2}{4 \cdot \frac{2}{15}} - 2 = \frac{-8}{49}.$$

Correspondingly,  $y_3 = \frac{1}{7}(-\frac{8}{49} - 1) + \frac{7}{15} = \frac{1546}{5145}$ . Therefore,  $2P = (-\frac{8}{49}, -\frac{1546}{5145})$ .

Now, the line joining  $P$  and  $2P$  has slope  $m = \frac{3947}{5985}$ . It intersects  $(E)$  again at a point with  $x$ -coordinate

$$\frac{1 - (\frac{3947}{5985})^2}{4 \cdot \frac{2}{15}} - 1 - \left(-\frac{8}{49}\right) = \frac{10858}{48735}.$$

This is the  $x$ -coordinate of the point  $3P$ . It also means that with  $t_1 = \frac{10858}{48735}$ , the system of equations

$$\begin{cases} t_1 t_2 t_3 = k, \\ t_1(t_2 + t_3) + t_2 t_3 = 1 \end{cases}$$

has rational solutions. In fact,

$$t_1 = \frac{10858}{48735}, \quad t_2 = \frac{3477}{7921}, \quad t_3 = \frac{5073}{3721}.$$

From these, we have a triangle with sides  $(\frac{2180}{5429}, \frac{36313}{52155}, \frac{68653}{76095})$ , semiperimeter 1, and area  $\frac{2}{15}$ . Magnifying 4641795 times, we obtain the Heron triangle

$$(1863900, 3231857, 4187833; 4641795, 2872834776270).$$

The given triangle (5, 12, 13), magnified 309453 times, gives

$$(1547265, 3713436, 4022889; 4641795, 2872834776270)$$

of the same semiperimeter and area.



# Exercises

**Problem A1.** (a) Prove that there is no Pythagorean triangle with one side of length  $\leq 2$ .

(b) Given an integer  $n \geq 3$ , construct a Pythagorean triangle with one leg of length  $n$ .

**Problem A2.** (a) Show that the hypotenuse of a Pythagorean triangle cannot be congruent to  $3 \pmod{4}$ .

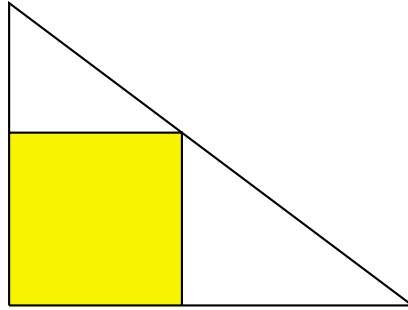
(b) For  $n \leq 30$ , determine if there is a Pythagorean triangle with hypotenuse  $n$ . If so, give an example.

$n$	$(a, b, c)$
1	none
2	none
4	none
5	(3, 4, 5)
6	
8	
9	
10	
12	
13	
14	
16	

$n$	$(a, b, c)$
17	
18	
20	
21	
22	
24	
25	
26	
28	
29	
30	(18, 24, 30)

(c) Make a conjecture: which integers  $n$  can be realized as the hypotenuse of a right triangle?

**Problem A3.** How many matches of equal length are required to make up the following configuration?



**Problem A4.** (a) Verify that  $(a^2 + b^2)(x^2 + y^2) = (ax - by)^2 + (bx + ay)^2$ .

(b) Make use of (a) to express 481 as a sum of two squares in two different ways.

(c) Find all Pythagorean triangles  $(a, b, c)$  with  $a < b$  and  $c = 481$ . Which of these are primitive?

**Problem A5.** Let  $(a, b, c)$  be a Pythagorean triple. Prove that

(a) at least one of  $a, b, c$  is divisible by 5;

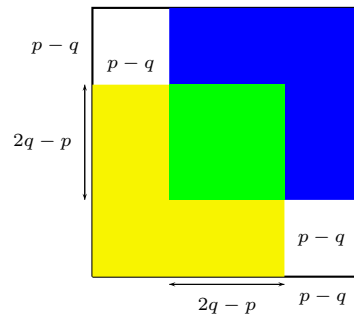
(b)  $abc$  is divisible by 60.

**Problem A6.** Each of the following is a prime of the form  $4k + 1$ .

Write it as a sum of two squares, and find the primitive Pythagorean triangle with this as hypotenuse.

$p$	$u^2 + v^2$	shorter sides
10009	$100^2 + 3^2$	9991, 600
10037		
10061		
10069		
10093		
10133		
10141		
10169		
10177		
10181		
10193		

**Problem A7.** Make use of the following diagram to prove the irrationality of  $\sqrt{2}$ .

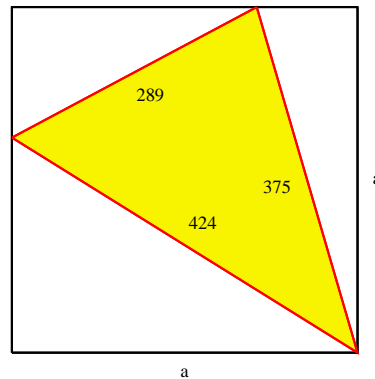


(c) Irrationality of  $\sqrt{2}$

**Problem A8.** Let  $p$  and  $q$  be positive integers such that the two quadratics  $x^2 - px + q$  and  $x^2 - px - q$  can both be factored (with integer

coefficients). Show that  $p$  and  $q$  are respectively the hypotenuse and the area of a Pythagorean triangle.

**Problem A9.** Here is the smallest square which can be dissected into three Pythagorean triangles and one with integer sides and integer area.



- (a) What is the length of a side of the square?
- (b) What are the lengths of the sides of the Pythagorean triangles?

**Problem A10 (Optional).**

perimeter	$m + n$	$2m$	$m$	$n$	$a$	$b$	$c$
1716	33						
	39						
14280	85						
	105						
	119						
317460	407						
	429						
	481						
	555						
1542684	899						
	957						
	1023						
	1131						
	1209						
6240360	1785						
	1955						
	1995						
	2185						
	2261						
	2415						
19399380	3135						
	3315						
	3553						
	3705						
	3927						
	4199						
	4389						

**Problem A11 (Optional).** In a class in Number Theory the professor gave four students the assignment of finding a fairly large primitive Pythagorean triangle using the well known formula for the legs:

$$A = 2mn, \quad B = m^2 - n^2, \quad C = m^2 + n^2,$$

where  $m$  and  $n$  are coprime integers, not both odd. The four students produced four entirely different primitive triangles, but on comparing them it was found that two of them had the same perimeter, while the other two also had the same perimeter, this perimeter differing from the

first one by 2. This interested the class greatly, and much time was spent in an effort to find other such sets, only to discover that there were only four such sets with perimeters less than 500,000. Can you find at least one such set ?

perimeter	$m + n$	$2m$	$m$	$n$	$a$	$b$	$c$
117390	273						
	301						
117392	253						
	319						
313038	459						
	527						
313040	455						
	559						
339150	425						
	475						
	525						
339152	451						
	517						
371448	469						
	603						
371450	437						
	475						
	575						

**Problem A12 (Optional).** Cross number puzzle on primitive Pythagorean triples.

1B, 3D, 9B	29B, 7A, 21D	12B, 11U, 20U
2D, 6D, 5B	19U, 15D, 7D	22D, 18B, 15U
27A, 2D, 26D	20A, 8D, 8A	16A, 31A, 33A
5D, 3A, 25B	30D, 14A, 9A	16B, 24D, 23B
28D, 35A, 3U	30U, 9U, 13D	22A, 32U, 32D
4U, 21A, 21D	19U, 17D, 10A	32U, 34A, 33A

1	2	3		4	5		6
7			8			9	
	10	11		12	13		
14	15	16		17	18		19
20			21			22	
	23	24		25	26		
27	28	29		30	31		32
33			34			35	

The answers are distinct 2- and 3-digit decimal numbers, none beginning with zero. Each of the above sets of answers is a primitive Pythagorean triple, in increasing size, so that the third member is the hypotenuse.

$A$  = across,  $B$  = back,  $D$  = down,  $U$  = up.

For example,  $1B$  has its tens and units digits in the squares labeled 2 and 1 respectively;  $11U$  is a 3-digit number with its tens and units digits in squares 16 and 11 respectively.

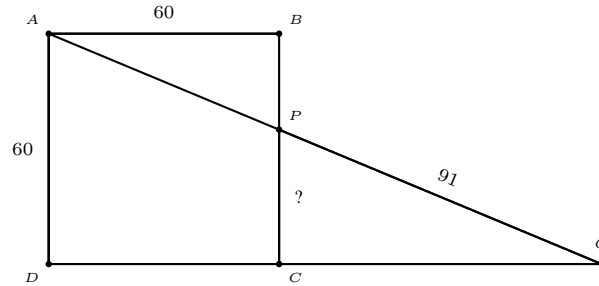
**Problem B1.** (a) Find an integer right triangle such that the hypotenuse *minus* each of the sides gives a cube.

(b) Find an integer right triangle such that the hypotenuse added to each of the sides gives a cube.<sup>1</sup>

**Problem B3.** A man has a square field, 60 feet by 60 feet, with other property adjoining the highway. He put up a straight fence in the line of 3 trees, at  $A$ ,  $P$ ,  $Q$ . If the distance between  $P$  and  $Q$  is 91 feet, and that from  $P$  to  $C$  is an exact number of feet, what is this distance?

**Problem B4.** Find the general form of a primitive Pythagorean triangle whose perimeter is a square. Give the smallest one.

<sup>1</sup>These two problems appeared in Diophantus' *Arithmetica*.



**Problem B5.** Find the shortest perimeter common to two different primitive Pythagorean triangles.

**Problem B6.** Solve the equation  $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$  in positive integers.

**Problem B7.** It is known that the inradius  $r$  of a triangle with sides  $(a, b, c)$  is given by  $r^2 = \frac{(s-a)(s-b)(s-c)}{s}$ , where  $s = \frac{1}{2}(a + b + c)$ . Determine all integer triangles with inradius 1.

**Problem B8.** The area  $\Delta$  of a triangle with sides  $a, b, c$  is given by the Heron formula

$$\Delta^2 = s(s-a)(s-b)(s-c),$$

where  $s = \frac{1}{2}(a + b + c)$ . Determine all integer triangles with area equal to perimeter.

**Problem B9.** Let  $a, b, c \in \mathbb{Z}$ . Prove that the line  $ax + by = c$  is tangent to the unit circle  $x^2 + y^2 = 1$  if and only if  $a^2 + b^2 = c^2$ .

**Problem B10.** For each natural number  $n$ , how many Pythagorean triangles are there such that the area is  $n$  times the perimeter? How many of these are primitive?

**Problem B11 (Optional).** Show that there are an infinite number

of Pythagorean triangles whose hypotenuse is an integer of the form  $3333 \dots 3$ .

**Problem B12 (Optional).** A lattice triangle is one whose vertices have integer coordinates. Determine all lattice triangles whose sides are tangent to the unit circle  $x^2 + y^2 = 1$ .

**Problem C1.** Find a parametrization of the rational points on the circle  $x^2 + y^2 = 2$ .

**Problem C2.** For each of the following equations, find a solution in small positive integers.

Equation	Positive integer solution $(x, y)$
$x^2 - 2y^2 = -1$	$(1, 1)$
$x^2 - 2y^2 = 1$	$(3, 2)$
$x^2 - 3y^2 = 1$	
$x^2 - 5y^2 = -1$	
$x^2 - 5y^2 = 1$	
$x^2 - 7y^2 = 1$	
$x^2 - 8y^2 = 1$	
$x^2 - 10y^2 = -1$	
$x^2 - 10y^2 = 1$	
$x^2 - 11y^2 = 1$	
$x^2 - 12y^2 = 1$	
$x^2 - 13y^2 = -1$	
$x^2 - 13y^2 = 1$	

**Problem C3.** (a) For each of the integers  $n = 5, \dots, 34$ , write, if possible,  $n$  as a sum of consecutive integers.

$n =$ sum	$n =$ sum	$n =$ sum
$5 = 2 + 3$	$6 = 1 + 2 + 3$	$7 = 3 + 4$
$8 =$	$9 =$	$10 =$
$11 =$	$12 =$	$13 =$
$14 =$	$15 =$	$16 =$
$17 =$	$18 =$	$19 =$
$20 =$	$21 =$	$22 =$
$23 =$	$24 =$	$25 =$
$26 =$	$27 =$	$28 =$
$29 =$	$30 =$	$31 =$
$32 =$	$33 =$	$34 =$

(b) Make a conjecture on the condition of a positive integer being a sum of consecutive integers (more than one).

(c) Can you prove your conjecture?

**Problem C4.** Find all rational points on the curve  $x^2 - 2y^2 - 4x - 4y + 2 = 0$ .

**Problem C5.** For each of the following conics, either find a rational point or prove that there are no rational points.

1.  $x^2 + y^2 = 6$ .

2.  $3x^2 + 5y^2 = 4$ .

3.  $3x^2 + 6y^2 = 4$ .

**Problem D1.**

Accompanying each prime  $p \equiv 1 \pmod{4}$  below is a square root  $q$  of  $-1 \pmod{p}$  with  $q^2 + 1 = mp$ . Make use of this information and follow Euler's proof to write  $p$  as a sum of two squares.

$p$	$q$	$m$
7937	1962	485
7993	2110	557
8017	1813	410
8069	2732	925
8089	2293	650

**Problem D2.**

For each of the following primes  $p \equiv 1 \pmod{4}$ , write  $p$  as a sum of two squares of integers by easy inspection. Make use of this to find a square root of  $-1 \pmod{p}$ .

$p$	$x^2 + y^2$	square root of $-1 \pmod{p}$
13	$3^2 + 2^2$	
73		
97		
113		
137		
149		
157		
173		
181		

**Problem D3.** Use Gauss' lemma to compute the Legendre symbol  $\left(\frac{7}{31}\right)$ .

**Problem D4.** Show that  $-3$  is a quadratic residue of  $p$  if and only if  $p = 6n + 1$ .

**Problem D5.** Show that  $5$  is a quadratic residue of all primes of the forms  $10n \pm 1$ , and a quadratic nonresidue of all primes of the form  $10n \pm 7$ .

**Problem D6.** In each of the following cases decide by calculating a Legendre symbol if the congruence is solvable. If so, find the solutions.

(a)  $x^2 \equiv -11 \pmod{59}$ ;

(b)  $x^2 \equiv 7 \pmod{83}$ ;

(c)  $x^2 \equiv 73 \pmod{127}$ ;

(d)  $x^2 \equiv 11 \pmod{37}$ .

**Problem D7.** Show that 6 is a quadratic residue mod 101 and calculate its square roots.

**Problem E1.** Find the square root of 2 modulo  $p$  for

1.  $p = 17$

2.  $p = 19$

3.  $p = 23$

**Problem E2.** Let  $p$  be an odd prime. Show that 5 is a quadratic residue modulo  $p$  if and only if  $p \equiv 1, 3, 7, 9 \pmod{20}$ .

**Problem E3.** For each of the following primes, decide if 5 is a quadratic residue modulo  $p$ . If so, find a square root of 5  $\pmod{p}$ .

1.  $p = 17$

2.  $p = 19$

3.  $p = 23$

4.  $p = 29$

**Problem E4.** Solve the congruences

(a)  $x^2 \equiv 30 \pmod{113}$ . (b)  $x^2 \equiv 7 \pmod{113}$ .

**Problem E5.** (a) Write down the quadratic residues modulo 11.

(b) For each of the quadratic residue  $a$  modulo 11, find two solutions of the congruence  $x^2 \equiv a \pmod{11}$ .

**Problem F1.**

Let  $a$  be a positive integer. Find the continued fraction expansion of  $\sqrt{a^2 + 1}$  and exhibit its periodicity.

**Problem F2.**

Let  $a$  be a positive integer. Find the continued fraction expansion of  $\sqrt{a^2 + a}$  and exhibit its periodicity.

**Problem F3.** Find the continued fraction expansion of  $\sqrt{29}$  and exhibit its periodicity.

**Problem F4.** Find the continued fraction expansion of  $\sqrt{44}$  and exhibit its periodicity.

**Problem F5.** Find the continued fraction expansions of the following quadratic irrationalities:

$$(i) \frac{1}{4}(\sqrt{5} + 1), \quad (ii) \sqrt{51}, \quad (iii) \sqrt{71}.$$

**Problem F6.** Let  $d = 14$ . Determine

- (i) the continued fraction expansion of  $\sqrt{d}$ ;
- (ii) the fundamental solution of the Pell equation  $x^2 - dy^2 = 1$ ;
- (iii) the complete solution of the Pell equation  $x^2 - dy^2 = 1$  in the form of a recurrence relation;

(iv) the second and third smallest solution of the equation  $x^2 - dy^2 = 1$ .

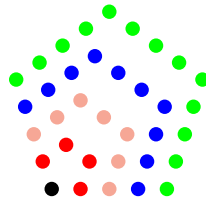
**Problem F7.** Let  $d = 13$ . Determine

- (i) the continued fraction expansion of  $\sqrt{d}$ ;
- (ii) the fundamental solution of the Pell equation  $x^2 - dy^2 = 1$ ;
- (iii) the complete solution of the Pell equation  $x^2 - dy^2 = -1$  in the form of a recurrence relation;
- (iv) the second and third smallest solution of the equation  $x^2 - dy^2 = -1$ .

**Problem F8.** The  $n$ -th triangular number is given by  $T_n = \frac{1}{2}n(n+1)$ . Find all integers  $n$  for which the sum of the  $(n-1)$ -st, the  $n$ -th, and the  $(n+1)$ -st triangular numbers is a square.

**Problem F9.** The pentagonal numbers are the sums of the arithmetic progression

$$1 + 4 + 7 + \cdots + (3n - 2) + \cdots$$



The  $n$ th pentagonal number is  $P_n = \frac{1}{2}n(3n - 1)$ . Find all integers  $n$  for which  $P_n$  is a square.

**Problem F10.**

1. A developer wants to build a community in which the  $n$  (approximately 100) homes are arranged along a circle, numbered consecutively from 1, 2,  $\dots$ ,  $n$ , and are separated by the club house, which is not numbered. He wants the house numbers on one side of club

house adding up to the same sum as the house numbers on the other sides. Between which two houses should he build the club house? How many houses are there altogether?

2. Later the developer finds out that government law requires the club house also has to be numbered. If he wants to maintain equal house number sums on both sides, he finds that he has to build significantly fewer homes. How many homes should he build, and what is the number of the club house?



# Bibliography

- [AZ] M. Aigner and G. M. Ziegler, *Proofs from the BOOK*, Springer, 1999.
- [And] G. E. Andrews, *Number Theory*, 1971; Dover reprint, 1994.
- [Ble] A. H. Bleiler, *Recreations in the Theory of Numbers*, Dover, 1966.
- [Cas] J. W. S. Cassels, *Lectures on Elliptic Curves*, LMS Student Texts 24, Cambridge University Press, 1991.
- [DSV] G. Davidoff, P. Sarnak, and A. Valette, *Elementary Number Theory, Group Theory, and Ramanujan Graphs*, LMS Student Texts 55, Cambridge University Press, 2003.
- [Dic] L. E. Dickson, *History of the Theory of Numbers*, 3 volumes, Chelsea; Dover reprint.
- [Gro] E. Grosswald, *Representations of Integers as Sums of Squares*, Springer-Verlag, 1985.
- [Guy] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd edition, 2004, Springer.
- [HK] A. Hurwitz and N. Kritikos, *Lectures on Number Theory*, Springer-Verlag, 1986.
- [Lev] W. LeVeque, *Fundamentals of Number Theory*, 1977; Dover reprint, 1996.
- [OLD] C. D. Olds, A. Lax, and G. Davidoff, *The Geometry of Numbers*, Anneli Lax New Mathematical Library, volume 41, MAA, 2000.
- [Rob] J. Roberts, *Elementary Number Theory, A Problem Oriented Approach*, MIT Press, 1977.

- [SO] W. Scharlau and H. Opolka, *From Fermat to Minkowski*, Springer-Verlag, 1984.
- [ST] I. Stewart and D. O. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, 3rd edition, AK-Peters, 2001.
- [Tat] J. J. Tattersall, *Elementary Number Theory in Nine Chapters*, 2nd edition, Cambridge, 2005.
- [Wei] A. Weil, *Number Theory, An approach through history, from Hammurapi to Legendre*, Birkhäuser, 1984.

## [Articles]

- [1] R. A. Beauregard, No arithmetic cyclic quadrilaterals, *College Math. Journal*, 37 (2006) 110–113.
- There is no cyclic quadrilateral whose sides are integers in arithmetic progression and whose area is an integer. This is a consequence of Euler's theorem that the product of four distinct nonzero integers in arithmetic progression cannot be a square.
- [2] R. A. Beauregard and K. D. Zelator, Perfect cyclic quadrilaterals, *Math. Mag.*, 7 (2002) 138–143.
- [3] L. E. Dickson, Lowest integers representing sides of a right triangle, *Amer. Math. Monthly*, 1 (1894) 6–11.
- [4] T. Erdélyi, On the equation  $a(a+d)(a+2d)(a+3d) = x^2$ , *Amer. Math. Monthly*, 107 (2000) 166–169.
- [5] K. Fogarty and C. O'Sullivan, Arithmetic progressions with three parts in prescribed ratio and a challenge of Fermat, *Math. Mag.*, 77 (2004) 389–391.
- [6] A. Hall, Geneology of Pythaogean triads, *Math. Gazette*, 54 (1970) 377–379.
- [7] P Hilton and J. Pedersen, Casting out nines revisited, *Math. Mag.*, 54 (1981) 195–201.
- [8] J. A. Holdener, Conditions equivalent to the existence of odd perfect numbers, *Math. Mag.*, 79 (2006) 389–391.
- [9] I. Kleiner, Fermat: the founder of modern number theory, *Math. Mag.*, 78 (2005) 3–14.
- [10] H. Klostergaard, Tabulating all Pythagorean triples, *Math. Mag.*, 51 (1978) 226–227.
- [11] L. P. Markov, Pythagorean triples and the problem  $A = mP$  for triangles, *Math. Mag.*, 79 (2006) 114–121.
- [12] R. B. McNeill, Square roots of  $-1$ , *Math. Mag.*, 51 (1978) 244.
- [13] P. S. Park, Ramanujan's continued fraction for a puzzle, *College Math. Journal* 36 (2005) 363–365.
- [14] J. Poet and D. L. Vestal Jr., Curious consequences of a miscopied quadratic, *College Math. Journal*, 36 (2005) 273–277.

- 
- [15] I. Richards, Continued fractions without tear, *Math. Mag.*, 54 (1981) 163–171.
- [16] F. Saidak, A new proof of Euclid’s theorem, *Amer. Math. Monthly*, 113 (2006) 937–938.
- [17] P. J. Schillo, On primitive Pythagorean triangles, *Amer. Math. Monthly*, 58 (1951) 30–32.
- [18] S. Szabó, A paper-and-pencil gcd algorithm for Gaussian integers, *College Math. Journal* 36 (2005) 374–380.
- [19] P. Ungar, Irrationality of square roots, *Math. Mag.*, 79 (2006) 147–148.
- [20] P. W. Wade and
- [21] A. Wayne, A genealogy of  $120^\circ$  and  $60^\circ$  natural triangles, *Math. Mag.*, 55 (1982) 157–162.
- [22] P. Yiu, Heronian triangles are lattice triangles, *Amer. Math. Monthly*, 108 (2001) –.
- [23] A. Zelevinsky, Visibles revisited, *College Math. Journal*, 36 (2005) 289–300.

**[More remote references]**

- [24] M. D. Hirschhorn, Triangles with integer sides, *Math. Mag.*, 76 (2003) 306–308.
- [25] I. G. Laukó, G. A. Pintér, and L. Pintér, Another step further . . . on a problem of the 1988 IMO, *Math. Mag.*, 79 (2006) 45–53.
- [26] M. Manea, Some  $a^n \pm b^n$  problems in number theory, *Math. Mag.*, 79 (2006) 140–145.