Math 104B: Number Theory II (Winter 2015)

Alina Bucur

Contents

1 Review

1.1 Prime numbers

A prime number p has the following properties:

- p has no other divisors than 1 and p;
- $p \mid ab \implies p \mid a$ or $p \mid b$.

There are infinitely many primes. Every positive integer can be written uniquely as a product of primes.

1.2 Euclidean algorithm

The algorithm is used to find the *greatest common divisor* $d = (a, b)$ of two positive integers a and b. It also can be used to find integers r, s such that

$$d = ar + bs.$$

1.3 Congruences

Definition. *We say that two integers a and b are* congruent modulo *some integer n and write $a \equiv b \pmod{n}$ if $n \mid a - b$. (That is to say, a and b give the same remainder when divided by n.)*

Here a few properties of congruences:

- $a \equiv a \pmod{n}$
- $a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$
- $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$
- $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n} \implies a \pm c \equiv b \pm d \pmod{n}, ac \equiv bd \pmod{n}$.
- $(a, n) = d$ and $ab \equiv ac \pmod{n} \implies b \equiv c \pmod{\frac{n}{d}}$.
- Given integers a and n, the equation $ax \equiv b \pmod{n}$ has solutions if $(a, n) \mid b$. Therefore it has solutions for all b iff $(a, n) = 1$. That is to say, if there exists an integer c such that $ac \equiv 1 \pmod{n}$. If such a c exists, it is unique modulo n, and the solution is $x = bc \pmod{n}$ is also unique modulo n.
- $a^{\phi(n)} \equiv 1 \pmod{n}$.

In addition to all these similarities to normal arithmetic operations (addition, subtraction, multiplication, division), there are similarities to linear algebra as well. For instance, the system of linear congruences

$$\begin{cases} a_{11}x_1 + \ldots + a_{1r}x_r \equiv b_1 \pmod{n} \\ \vdots \\ a_{r1}x_1 + \ldots + a_{rr}x_r \equiv b_r \pmod{n} \end{cases}$$

has unique solution $\pmod{n}$ iff $\det(a_{ij})$ and n are coprime.

Theorem 1.1 (Chinese Remainder Theorem)**.** *Assume that $m_1, \ldots, m_r$ are positive integer with the property that any two of them are relatively prime. Then, for any $a_1, \ldots, a_r \in \mathbb{Z}$, the system of equations*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

has a unique solution $\pmod{m_1 \ldots m_r}$.

1.4 Groups

Definition. *A group G is a set endowed with an operation $\circ : G \times G \to G$ with following properties.*

(*i*) *$x \circ (y \circ z) = (x \circ y) \circ z$ for all $x, y, z \in G$ (associativity).*

(*ii*) *There exists an element $e \in G$ (called the unit of the group) such that $x \circ e = e \circ x = x$ for all $x \in G$.*

(*iii*) *For each $x \in G$ there exists an element $x^{-1} \in G$ (the inverse of x) such that*

$$x \circ x^{-1} = x^{-1} \circ x = e.$$

Definition. *We say that a group G is abelian (commutative) if $x \circ y = y \circ x$ for all $x, y \in G$.*

Theorem 1.2 (Lagrange)**.** *In a finite group G the order of every element is a divisor of the order of the group $\#G$. In particular*

$$x^{\#G} = e \text{ for all } x \in G.$$

Two particular cases are the following result in modular arithmetic.

Theorem 1.3 (Fermat)**.** *If p is a prime and a an integer not divisible by p, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Theorem 1.4 (Euler)**.** *If a and n are relatively prime nonzero integers, then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

1.5 Primitive roots

A primitive root modulo n is a generator of the group U_n of the units modulo n. That is, a is a primitive root modulo n if and only if its order in U_n is exactly $\phi(n)$, i.e. $\phi(n)$ is the smallest positive integer m such that

$$a^m \equiv 1 \pmod{n}.$$

2 Powers and roots in modular arithmetic

To calculate powers modulo n one can use Euler's theorem. For instance, let us compute $7^{42} \pmod{11}$. We will use the fact that $7^{10} \equiv 1 \pmod{11}$.

$$7^{42} \pmod{11} = 7^{4\cdot 10+2} \pmod{11} = (7^{10})^4 \cdot 7^2 \pmod{11} = 7^2 \pmod{11} = 5 \pmod{11}.$$

The above works for any integer $n > 1$. For roots, we will restrict ourselves to computing roots modulo primes.

To compute roots modulo a *prime* p, one could use a primitive root.

Example 2.1. Find a third root of 5 modulo 11.

That is, we want to find x such that

$$x^3 \equiv 5 \pmod{11}.$$

We know that 2 is a primitive root modulo 11. Indeed, here's a table of the powers of 2 modulo 11.

n	1	2	3	4	5	6	7	8	9	10
$2^n \pmod{11}$	2	4	8	5	10	9	7	3	6	1

We see that $5 = 2^4 \pmod{11}$. Thus we want to solve

$$x^3 \equiv 2^4 \pmod{11}.$$

Since 2 is a primitive root, we know that $x \equiv 2^y \pmod{11}$ for some y. Thus our equation becomes

$$2^{3y} \equiv 2^4 \pmod{11} \iff 2^{3y-4} \equiv 1 \pmod{11} \iff 3y - 4 \equiv 0 \pmod{10}$$

$$\iff 3y \equiv 4 \pmod{10} \iff y \equiv 8 \pmod{10}.$$

We managed to complete the last step because $(3, 10) = 1$ so 3 has an inverse modulo 10. Thus our solution is

$$x \equiv 2^8 \pmod{11} \equiv 3 \pmod{11}.$$

The above works for any integer $n > 1$. Namely, given $(a, n) = 1$ we would like to find x such that

$$x^k \equiv a \pmod{n}.$$

If we have a primitive root g modulo n we express $a \equiv g^b \pmod{n}$ and $x \equiv g^y \pmod{n}$ and our equatioon becomes

$$g^{ky} \equiv g^b \pmod{n} \iff ky \equiv \pmod{\phi(n)}.$$

If k and $\phi(n)$ are relatively prime, then we can find such a y which in turn leads us to x. In particular, we observe the following.

Remark 2.2. If k and $\phi(n)$ are relatively prime, then every integer a coprime to n has a kth root modulo n.

However, primitive roots are not easy to find, especially when we deal with large numbers. And in addition to finding a primitive root, the above method also requires another nontrivial computation, namely we have to find b such that $a \equiv g^b \pmod{n}$. If we restrict our attention to roots modulo *primes*, one can find a shortcut using Fermat's theorem.

Example 2.3. Find the fifth root of 2 modulo 17.

By Fermat's theorem we know that

$$2^{16} \equiv 1 \pmod{17}$$

and

$$2^{17} \equiv 2 \pmod{17}.$$

We can multiply these two relations and get that

$$2^{33} \equiv 2 \pmod{17}.$$

Multiply again by 2^{16} and get

$$2^{49} \equiv 2 \pmod{17}.$$

We will repeat the operation of multiplying by 2^{16} until we get an exponent that is a multiple of 5. Fortunately, we do not have to go far, as the next iteration yields

$$2^{65} \equiv 2 \pmod{17}.$$

Thus

$$2 \equiv 2^{65} \pmod{17} \equiv 2^{5 \cdot 13} \pmod{17} \equiv (2^1 3)^5 \pmod{17}$$

, so $x \equiv 2^1 3 \pmod{17}$. In order to compute this, we write 13 as a sum of powers of 2 (since squaring saves time), i.e. $13 = 8 + 4 + 1$.

We have

$$2^1 \equiv 2 \pmod{17}, \quad 2^2 \equiv 4 \pmod{17},$$
$$2^4 \equiv 16 \pmod{17} \equiv -1 \pmod{17}, \quad 2^8 \equiv 1 \pmod{17}.$$

Thus,

$$2^{13} \equiv 2^8 \cdot 2^4 \cdot 2^1 \pmod{17} \equiv 1 \cdot (-1) \cdot 2 \pmod{17} \equiv 15 \pmod{17}$$

is a fifth root of 2 modulo 17.

In general, suppose that we want to compute the kth root of a number $a \not\equiv 0 \pmod{p}$ for some prime p. Fermat's theorem tells us that $a^{p-1} \equiv 1 \pmod{p}$, so we can write a as a power of itself by multiplying it by a^{p-1} over and over again:

$$a \equiv a^p \equiv a^{2p-1} \equiv a^{3p-2} \equiv \ldots \pmod{p},$$

i.e.

$$a \equiv a^{\ell(p-1)+1} \pmod{p} \text{ for all } \ell.$$

If we can find m such that $mk = \ell(p-1) + 1$ for some ℓ, then we would get $a \equiv a^{mk} \pmod{p}$, so $x \equiv a^m \pmod{p}$ is a kth root of a modulo p.

Note that we can always find such an m provided that $(k, p-1) = 1$. In fact, in this case, we can find m via the Euclidean algorithm.

How to find the kth root of a modulo p

- Check that p is a prime, $p \nmid a$ and that k is relatively prime to $p-1$. If any of these conditions fails, the process will not work. In fact, the kth root might not exist.
- Use the Euclidean algorithm to find positive integers m and ℓ such that

$$mk = \ell(p-1) + 1.$$

- Then $(a^m)k \equiv a^{\ell(p-1)+1} \equiv a \pmod{p}$, so a^m is a kth root of a modulo p.
- Evaluate $x \equiv a^m \pmod{p}$.
- **Check!** Calculate $x^k \pmod{p}$ and verify that you indeed get a.

It would be a good exercise to figure out how to modify this algorithm for modular arithmetic modulo some general positive integer $n > 1$ instead of a prime p.

3 Classical crypto systems

3.1 Caesar shifts

Named after Julius Caesar, these codes require a "shift" of the letters. For instance, a Caesar shift of $+1$ takes

$$A \to B \to C \to \cdots \to Z \to A.$$

For instance, in this encoding,

THIS CODE IS DUMB

becomes

UIJT DPEF JT EVNC.

A Caesar shift of $+3$ would take $A \to D$, $B \to E$, and so forth. A shift of -1 would take $A \to Z \to Y \to \cdots \to C \to B \to A$. Such a code is easy to break by trying various shifts on just the first few letters until we get something that makes sense.

An even simpler shift would just assign each letter a number encoding its position in the alphabet. That is, $A \to 1, B \to 2, \ldots, Z \to 26$. So the message

EVEN WORSE

becomes

522514 231518195.

Needless to say, this is also easy to decode.

3.2 Permutation codes

A version of this code was used by the Spartans. The idea is to use a rectangle of given dimension $(m \times n)$, and write the message horizontally in the rectangle, but read it vertically.

Let us say that we want to encode the message

IT IS THURSDAY AND THE WEATHER IS BEAUTIFUL

using a 3×5 permutation code. We write the beginning of the message in a rectangle of the given dimension

I	T	I	S	T
H	U	R	S	D
A	Y	A	N	D

and then we continue with another rectangle and so on:

T	H	E	W	E
A	T	H	E	R
I	S	B	E	A

. . .

The encoded message is read vertically:

IHATUYIRASSNTDDTAIHTSEHBWEEERA . . .

The way to break this code is to read every second letter, then every third letter until the message begins to make sense. For instance, reading every second letter above gives

IAUIA . . .

and we need not go any further as this is gibberish. But when we try every third letter we get

ITIST . . .

and by now we are pretty confident that this is the key and we can go on to decipher the rest and recover the original text.

3.3 Vigenère code

Named after its inventor, Blaise de Vigenère, this cypher was considered unbreakable at the time. Indeed, it took centuries before an effective way of cracking it was discovered. It is a shift code, but with a twist. Namely, one chooses a key word, e.g. "TODAY". To encode the message

IT IS THURSDAY

one adds TODAYTODAYTODAY. . . to it modulo 26. Namely,

	I	T	I	S	T	H	U	R	S	D	A	Y
+	T	O	D	A	Y	T	O	D	A	Y	T	O

which becomes

	9	20	9	19	20	8	21	18	19	4	1	25	
+	20	15	4	1	25	20	15	4	1	25	20	15	
	3	9	13	20	19	2	10	22	20	3	21	14	(mod 26)

Thus, the encoding reads

CIMTSBJVTCUO.

To decode, one uses the key word again. That, is converts CIMTSBJVTCUO in numbers up to 26 and subtracts TODAY from it.

	3	9	13	20	19	2	10	22	20	3	21	14	
-	20	15	4	1	25	20	15	4	1	25	20	15	
	9	20	9	19	20	8	21	18	19	4	1	25	(mod 26)

The Vigenère code is harder to crack with the usual methods for cracking substitution codes. Since the letter E may be encoded in five different ways depending on where it appears

in the message, one cannot establish which symbol represents E by simply identifying the symbol which appears most often. But given a long enough message one can still profit by the same kind of frequency analysis. One would have to look at every other letter, then every 3rd letter, every 4th letter and so on and chart the frequency of the symbols. In our example above, we would see little variation in the frequency of the various symbols until we look at every 5th letter (the length of the key word). Then we would see dramatic changes in the frequencies. Once we have the length of the key word, we can perform the old frequency analysis taken this information into account.

4 More crypto systems

In order to use any mathematical encryption scheme, one must first find a universal way of encoding text into numbers. The first instance we saw of this was the one were each letter was assigned a number encoding its position in the Latin alphabet ($A \to 1, B \to 2, \ldots$). In order to use computers, it is convenient to view keys, plaintexts, and ciphertexts as numbers and to write those numbers in binary form. An encoding scheme is assumed to be entirely public knowledge and used by everyone for the same purposes. One such example is the ASCII code.

Using ASCII, a text may be viewed as a sequence of binary blocks, where each block consists of 8 bits, i.e., of a sequence of eight ones and zeros. A block of 8 bits is called a byte. For human comprehension, a byte is often written as a decimal number between 0 and 255. The full table of values can be found at `http://www.ascii-code.com/`, but for our purposes we will only need the printable code chart from `http://en.wikipedia.org/wiki/ASCII`. Here are a few examples

Character	*Decimal*	*Binary*	*Character*	*Decimal*	*Binary*
	32	00100000	0	48	00110000
(	40	00101000	1	49	00110001
)	41	00101001	⋮		
,	44	00101100	9	57	00111001
.	46	00101110			
=	61	00111101			

and

Character	*Decimal*	*Binary*	*Character*	*Decimal*	*Binary*
A	65	01000001	a	97	01100001
B	66	01000010	b	98	01100010
⋮			⋮		
Z	90	01011010	z	122	01111010

Once we have encoded the text into a number (or series of numbers), then we can proceed to talk about encryption. In general, one chooses a key k and for that we define an encryption

function e_k that transforms (plaintext) messages into cyphertext (i.e.$e_k(m) = c$ for a message m and a cyphertext c) and a decryption function d_k that takes cyphertexts and decrypts them into plaintext messages. From now on, we will use m to denote a plaintext message and c a cyphertext. So $e_k(m) = c$ and $d_k(c) = m$ are inverse functions.

Multiplication in modular arithmetic

One simple encryption function comes directly from modular arithmetic. Let p be a prime (large!, i.e. $> 2^{100}$) and we will choose our keys k, plaintexts m and cyphertexts c from the set

$$\{0, 1, \ldots, p-1\}.$$

The encryption function will be $e_k(m) = km \pmod{p}$ and decryption $d_k(c) = k^{-1}c \pmod{p}$.

Affine cypher

is a slight modification of the previous one where the key $k = (k_1, k_2)$ consists of two numbers modulo p and

$$e_k(m) = k_1 m + k_2 \pmod{p}, \quad d_k(c) = k_1^{-1}(c - k_2) \pmod{p}.$$

Hill cypher

This is a variation of the affine cypher where k_1 is an invertible $n \times n$ matrix with entries modulo p and k_2, m, c are n vectors modulo p. The formulas are the same.

5 Public key cryptography

All the codes mentioned before are *symmetric* codes, where both for encryption and decryption one needs the same key k. The problem is that both the sender and recipient (typically one calls them Alice and Bob) need to have the same key. But in public key cryptography, the two parties usually have never met (you and your bank or Amazon, etc.), they communicate only over the internet and they have to assume that someone (usually called Eve) could eavesdrop on their whole communication. So another system is necessary, one that ensures that Alice and Bob can communicate securely even Eve can see their whole correspondence. The first solution to this seemingly impossible task was proposed by Diffie and Hellman and is based on the so-called *discrete log problem*.

5.1 Discrete logarithm problem

The problem is simple to state. Given a (large) prime p, a primitive root g modulo p and $a \not\equiv 0 (\text{mod } p)$, find x such that $a \equiv g^x (\text{mod } p)$. We know that x exists, but if p is large it is very hard to find x. Basically, as soon as the brute force approach (compute all powers

of g until you find a among them) becomes unmanageable for a computer, the problem is unsolvable.

If we denote $x = \log_g(a)$ then this "discrete" log function has the same properties as the usual logarithm, e.g.

$$\log_g(1) = 0, \quad \log_g(ab) = \log_g(a) + \log_g(b).$$

5.2 Diffie-Hellman key exchange

The Diffie-Hellman key exchange algorithm solves the following dilemma. Alice and Bob want to share a secret key for use in a symmetric cipher, but their only means of communication is insecure. Every piece of information that they exchange is observed by their adversary Eve.

Step 1 (public) The first step is for Alice and Bob to agree on a large prime p and a nonzero integer g modulo p with larger order in U_p For the moment, say g is a primitive root modulo p. (In practice, it is best if they choose g such that its order in U_p is a large prime.) Alice and Bob make the values of p and g public knowledge; for example, they might post the values on their web sites, so Eve knows them, too.

Step 2 (private): Alice chooses $a (\text{mod } p)$ and Bob chooses $b (\text{mod } p)$.

Step 3 (private): Alice computes $A \equiv g^a (\text{mod } p)$ and Bob computes $B \equiv g^b (\text{mod } p)$.

Step 4 (public): Alice and Bob exchange the values A and B (Eve can see this).

Step 5 (private) Alice computes $B^a (\text{mod } p)$ and Bob computes $A^b (\text{mod } p)$. Note that both these values are equal to $k \equiv g^{ab} (\text{mod } p)$. This is their shared private key.

Note that if Eve can solve the discrete log problem (i.e. given A and B find a and b) then she can find k. It is nontrivial, but true, that finding k given A, B, g and p is as hard as solving DLP.

Example 5.1. Let $p = 941$ and $g = 627$ a primitive root in U_p. If $a = 347$ and $b = 781$ then

$$A \equiv 627^{347} \equiv 390 \pmod{941} \quad B \equiv 627^{781} \equiv 691 \pmod{941}$$

so

$$k \equiv 627^{347 \cdot 781} \equiv 470 \pmod{941}.$$

5.3 ElGamal public key crypto system

Although the Diffie-Hellman key exchange algorithm provides a method of publicly sharing a random secret key, it does not achieve the full goal of being a public key cryptosystem, since a cryptosystem permits exchange of specific information, not just a random string of bits. The Elgamal public key encryption algorithm is based on the discrete log problem and is closely related to Diffie-Hellman key exchange.

Step 1 (public) A trusted party chooses and publishes a large prime p and an element g modulo p of large (prime) order.

Step 2 (private) Alice chooses a private key $1 \leq a \leq p-1$ and computes $A \equiv g^a (\text{mod } p)$.

Step 3 (public) Alice publishes the public key A.

Step 4 (private) Bob chooses plaintext m and a random element k called *ephemeral key*. He will choose a different k each time he wants to send a message. Bob uses Alice's public key A and his ephemeral key k to compute

$$c_1 \equiv g^k \pmod{p}, \quad c_2 \equiv mA^k \pmod{p}.$$

Step 5 (public) Bob sends ciphertext $c = (c_1, c_2)$ to Alice. (Eve can see this.)

Step 6 Alice decrypts Bob's message by computing

$$m \equiv c_1^{-a} c_2 \pmod{p}.$$

5.4 RSA

Named after Ron Rivest, Adi Shamir and Leonard Adleman, this code (or variants of it) is used everywhere these days: ATMs, online transactions, even when we log in to get email from a remote location. The system uses a version of the discrete log problem modulo an integer $N = pq$ for two (large) primes p and q. The key consists of $k = (N, e)$. The encryption is

$$e_k(m) \equiv m^e \pmod{N}.$$

To decrypt we need to be able to recover from a cyphertext c the plaintext m such that $m^e \equiv c (\text{mod } N)$. That is, given N, c, and e we need to solve

$$x^e \equiv c \pmod{N}.$$

5.4.1 Powers and roots in modular arithmetic revisited

We want to find a way to solve

$$x^k \equiv c \pmod{n}$$

for an integer $n > 1$. We would like a version of the algorithm from Section 2 for finding kth roots modulo a prime, but in arithmetic modulo an arbitrary integer $n > 1$. In Section 2 we based our algorithm on Fermat's theorem, that is on the structure of U_p. Now we will use as a starting point Fermat's theorem

$$a^{\phi(n)} \equiv 1 \pmod{n} \text{ for all } (a, n) = 1.$$

That is, we will use the fact that U_n is cyclic. For that, we need to start with $c \in U_n$, i.e. c relatively prime to n. Then

$$c \equiv c^{\phi(n)+1} \equiv c^{2\phi(n)+1} \equiv c^{3\phi(n)+1} \equiv \ldots \pmod{n}.$$

If we find a number of the form $\ell\phi(n)+1$ that is also a multiple of k then we have $\ell\phi(n)+1 = dk$ for some d and

$$c \equiv c^{\ell\phi(n)+1} \equiv (c^d)^k.$$

Thus $x \equiv c^d \pmod{n}$ is a kth power of c modulo n.

Note that such a d exists if and only if k and $\phi(n)$ are relatively prime.

How to find the kth root of c modulo n

- Check that $n > 1$, $(n, c) = 1$ and that k is relatively prime to $\phi(n)$. If any of these conditions fails, the process will not work. In fact, the kth root might not exist.
- Use the Euclidean algorithm to find positive integers d and ℓ such that

$$dk = \ell\phi(n) + 1.$$

- Then $(c^d)^k \equiv c^{\ell(p-1)+1} \equiv c \pmod{n}$, so c^d is a kth root of c modulo n.
- Evaluate $x \equiv c^d \pmod{n}$.
- **Check!** Calculate $x^k \pmod{n}$ and verify that you indeed get c.

5.5 Back to RSA

The RSA public key system works as follows.

Step 1 (key creation, private) Bob chooses secret primes p and q. Computes $N = pq$. He also chooses the encryption exponent e that is a positive integer coprime to $\phi(N) = (p-1)(q-1)$.

Step 2 (public) Bob publishes N and e.

Step 3 (private, encryption) Alice chooses the plaintext m ad uses Bob's public key to encrypt it. That is, she computes the cyphertext

$$c \equiv m^e \pmod{N}.$$

Step 4 (public) Alice sends ciphertext c to Bob. (Eve can see this.)

Step 5 (private, decryption) Bob decrypts Alice's message by computing first

$$d \equiv e^{-1} \pmod{\phi(N)} \equiv e^{-1} \pmod{(p-1)(q-1)}$$

and then

$$m \equiv c^d \pmod{N}.$$

6 Method of descent

The method of descent relies on the fact that positive integers are well-ordered, i.e. any two can be compared and in any set of positive integers there is a smallest element (this is not true for integers, or for rational numbers). The first instance of descent that many people see is the long division. If we want to divide a positive integer a by another positive integer b, we can successively subtract b from a and obtain the sequence of integers

$$a > a - b > a - 2b > \dots$$

Since there are only finitely many integers between a and 0, there exists q such that $a - qb \geq 0 > a - (q+1)b$ and in this case $r = a - qb < b$.

This is in a nutshell the idea of descent: one starts with a positive integer with some property, then constructs a smaller positive integer with that same property and so on. Sometimes the descent works only so far and then the inequalities cease to be correct. In this case, either the process stops and we found what we were looking for as above; or one might have to check a certain range of numbers to see that there are no solutions in that range to the problem at hand. Sometimes one shows that starting with a solution, we can construct an infinite sequence of smaller and smaller positive integers, leading to a contradiction.

6.1 Pythagorean triples

We want to find all right triangles with all three sides of integral length. In other words, we want to solve the diophantine equation

$$x^2 + y^2 = z^2. \tag{6.1}$$

Note that any solution generates a positive solution by changing the sign, hence solving the equation in $\mathbb{Z}$ is equivalent to solving it in $\mathbb{Z}_{>0}$, which is the same as finding all right triangles with integral sides. We can further reduce the problem to finding solutions with $(x, y, z) = 1$, that is we exclude similar triangles. Each such solution will generate infinitely many solutions (dx, dy, dz) with gcd $= d$ and vice versa.

It is worth noticing that if a prime p divides two of the number x, y, z then it would have to divide the third one as well. Hence we must have $(x, y) = (y, z) = (x, z) = 1$.
There is one more observation we can make to simply our problem.

Claim $x \not\equiv y \pmod 2$.

Proof. We know that we cannot have $x \equiv y \equiv 0 \pmod 2$ because that force x and y to not be relatively prime. We are going to argue by contradiction for the other case as well. Assume that $x \equiv y \equiv 1 \pmod 2$. Then $x^2 \equiv y^2 \equiv 1 \pmod 4$, and this would mean that $z^2 \equiv 2 \pmod 4$, which is impossible. □

Since x and y are interchangeable in our problem, we can assume without loss of generality that x is odd and y is even. This also implies that z is odd. We can rewrite our equation as

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

and further as

$$\left(\frac{y}{2}\right)^2 = \frac{z - x}{2} \cdot \frac{z + x}{2}.$$

All the fractions above are really positive integers since y is even and x, z are both odd with $z > x$. Next we want to use the following observation.
Fact If $a, b, c \in \mathbb{Z}$ with $(a, b) = 1$ and $ab = c^2$, then there exist integers a_1, b_1 such that $a = a_1^2$ and $b = b_1^2$. Clearly a_1 and b_1 have to be relatively prime as well.

In order to do use this fact, we need to show that gcd $\left(\frac{z - x}{2}, \frac{z + x}{2}\right) = 1$. Assume that p is a prime that divides both of them. Then p divides both their sum and their difference, that is it has to divide both x and z. That would imply that p divides y as well, and this contradicts the fact that $(x, y, z) = 1$.

Hence the gcd of the two fractions is indeed 1 and there must exist positive integers u and v with $(u, v) = 1$ such that

$$\frac{z - x}{2} = v^2 \qquad \text{and} \qquad \frac{z + x}{2} = u^2.$$

This leads to

$$\begin{cases} x = u^2 - v^2 \\ y = 2uv \\ z = u^2 + v^2. \end{cases}$$

Note that since x and z are odd, we must also have $u \not\equiv v \pmod 2$. Also, $x > 0$ implies $u > v$.

In short, we proved that all positive Pythagorean triples are of the form

$$\begin{cases} x = d(u^2 - v^2) \\ y = 2duv \\ z = d(u^2 + v^2) \end{cases}$$

where $u, v \in \mathbb{Z}$, $u > v > 0$ and $u \not\equiv v \pmod 2$.

6.2 More descent

We want to study the Fermat equation for $n = 4$,

$$x^4 + y^4 = z^4. \tag{6.2}$$

Fermat himself proved that it has no non-trivial solutions (i.e. no integer solutions with $xyz \neq 0$). His proof uses again the method of descent.

Assume that x, y, z are positive integers satisfying (6.2). Set $d = (x, y, z)$. Then $x = dx_1$, $y = dy_1$ and $z = dz_1$ where $(x_1, y_1, z_1) = 1$ and x_1, y_1, z_1 are also positive integers satisfying the same equation (6.2). In particular, $x_1^2, y_1^2, t_1 = z_1^2$ is a relatively prime Pythagorean triple. In particular, x_1, y_1, t_1 are relatively prime positive integers that form a solution to the equation

$$X^4 + Y^4 = T^2. \tag{6.3}$$

Note that x_1 and y_1 are interchangeable, so we can assume without loss of generality that x_1 is odd and y_1 is even. It follows from our study of Pythagorean triples (Section 6.1) there exist integers $u > v > 0$ such that $(u, v) = 1$ and $u \not\equiv v \pmod 2$ such that

$$\begin{cases} x_1^2 = u^2 - v^2 \\ y_1^2 = 2uv \\ t_1 = u^2 + v^2. \end{cases} .$$

Since x_1 is odd, we have $x_1^2 \equiv 1 \pmod 4$ and therefore u is odd and v is even.

Note that this implies further that $(u, 2v) = 1$. Since $u(2v) = y_1^2$ and $2v$ is even, we have $u = t_2^2$ and $2v = 4d^2$ for some positive *relatively prime* integers t_2 and d, with t_2 odd.

We can rewrite the formula for x_1 as

$$x_1^2 + v^2 = u^2.$$

Since $(u, v) = 1$ it follows that x_1, v, u is a relatively prime Pythagorean triple with x_1 odd and v even. Applying again the results from Section 6.1, there exist integers $a > b > 0$ such

that $(a,b)=1$, $a \not\equiv b \pmod 2$ and

$$\begin{cases} x_1 = a^2 - b^2 \\ v = 2ab \\ u = a^2 + b^2. \end{cases} .$$

Since $v = 2ab$ and $2v = 4d^2$ it follows that $ab = d^2$. But $(a,b) = 1$ and therefore $a = x_2^2, b = y_2^2$ for some integers $x_2 > y_2 > 0$ with $(x_2, y_2) = 1$ and $x_2 \not\equiv y_2 \pmod 2$.

To recap, we have

$$\begin{aligned} u &= a^2 + b^2 \\ a &= x_2^2 \\ b &= y_2^2 \\ u &= t_2^2. \end{aligned}$$

Therefore x_2, y_2, t_2 are relatively prime positive integers that satisfy

$$x_2^4 + y_2^4 = t_2^2.$$

But we also have

$$t_2 \leq t_2^4 = u^2 < u^2 + v^2 = t_1.$$

We proved that if we start with a relatively prime positive solution (x_1, y_1, t_1) to (6.3) we can produce another relatively prime solution (x_2, y_2, t_2) with $0 < t_2 < t_1$. Applying this fact over and over again we obtain infinitely many positive solutions (x_n, y_n, t_n) to (6.3) with

$$0 < \ldots < t_n < t_{n-1} < \ldots < t_1.$$

This is impossible because there are only finitely many integers between 0 and t_1. (In fact, there are $t_1 - 1$ of them!)

In short, the assumption that we can find a positive solution to (6.2) led to a contradiction, and that proves that no such solution can exist.

7 Gaussian integers

The Gaussian integers $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ form a ring with respect to the usual addition and multiplication. Furthermore, it is an Euclidean ring with respect to the norm map $N : \mathbb{Z}[i] \to \mathbb{R}_{\geq 0}$ given by $N(x+iy) = x^2 + y^2 = |x+iy|^2 = (x+iy)(x-iy) = (x+iy)\overline{(x+iy)}$ where the absolute value is the one on $\mathbb{C}$ and the bar denotes the complex conjugate.

The norm map is clearly multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$. Moreover, $N(\alpha) = 0 \iff \alpha = 0$. It also allows us to perform long division and use the Euclidean algorithm to find the gcd of two elements exactly as in $\mathbb{Z}$.

The norm N gives $\mathbb{Z}[i]$ a euclidean ring structure. For more about Euclidean rings, see Chapter 2 of the textbook.

Theorem 7.1. *For any $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$ there exist $\gamma, \rho \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma + \rho$ and $0 \leq N(\rho) < N(\beta)$.*

Proof. Done in 104A or abstract algebra. □

Definition. *There is a notion of* divisibility *in a ring R that mirrors the notion from $\mathbb{Z}$. Namely, if $\alpha, \beta \in R$ we say that $\alpha \mid \beta$ if there exists $\gamma \in R$ such that $\beta = \alpha\gamma$.*

7.1 Units in $\mathbb{Z}[i]$

An element $x = a + bi \in \mathbb{Z}[i]$, $a, b \in \mathbb{Z}$ is a unit if there exists $y = c + di \in \mathbb{Z}[i]$ such that $xy = 1$. This implies

$$1 = |x|^2|y|^2 = (a^2 + b^2)(c^2 + d^2)$$

But a^2, b^2, c^2, d^2 are non-negative integers, so we must have

$$1 = a^2 + b^2 = c^2 + d^2.$$

This can happen only if $a^2 = 1$ and $b^2 = 0$ or $a^2 = 0$ and $b^2 = 1$. In the first case we obtain $a = \pm 1, b = 0$; thus $x = \pm 1$. In the second case, we have $a = 0, b = \pm 1$; this yields $x = \pm i$. Since all these four elements are indeed invertible we have proved that

$$U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}.$$

7.2 Primes in $\mathbb{Z}[i]$

An element $x \in \mathbb{Z}[i]$ is *prime* if it generates a prime ideal, or equivalently, if whenever we can write it as a product $x = yz$ of elements $y, z \in \mathbb{Z}[i]$, one of them has to be a unit, i.e. $y \in U(\mathbb{Z}[i])$ or $z \in U(\mathbb{Z}[i])$.

7.3 Rational primes p in $\mathbb{Z}[i]$

If we want to identify which elements of $\mathbb{Z}[i]$ are prime, it is natural to start looking at primes $p \in \mathbb{Z}$ and ask if they remain prime when we view them as elements of $\mathbb{Z}[i]$. If $p = xy$ with $x = a + bi, y = c + di \in \mathbb{Z}[i]$ then

$$p^2 = |x|^2|y|^2 = (a^2 + b^2)(c^2 + d^2).$$

Like before, $a^2 + b^2$ and $c^2 + d^2$ are non-negative integers. Since p is prime, the integers that divide p^2 are $1, p, p^2$. Thus there are three possibilities for $|x|^2$ and $|y|^2$:

1. $a^2 + b^2 = 1$ and $c^2 + d^2 = p^2$;
2. $a^2 + b^2 = p$ and $c^2 + d^2 = p$;

3. $a^2 + b^2 = p^2$ and $c^2 + d^2 = 1$.

In the first case, $a^2 + b^2 = 1 \implies x \in U(\mathbb{Z}[i])$. Similarly, in the third case $c^2 + d^2 = 1 \implies y \in U(\mathbb{Z}[i])$.

Therefore we have the following result.

Proposition 7.2. *A prime number $p \in \mathbb{Z}$ fails to be a prime element of $\mathbb{Z}[i]$ if and only if p can be written as the sum of two squares, i.e. $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}, a, b > 0$.*

We also have the following observation.

Lemma 7.3. *If a prime number p can be written as the sum of two squares, then $p = 2$ or $p \equiv 1 (\text{mod } 4)$.*

Proof. Assume $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$. We know that $a^2, b^2 \equiv 0, 1 (\text{mod } 4)$. Thus $a^2 + b^2 \equiv 0, 1, 2 (\text{mod } 4)$. Since p is prime, it cannot be divisible by 4. So we have either $p \equiv 2 (\text{mod } 4)$ (and in this case $p = 2$) or $p \equiv 1 (\text{mod } 4)$.

□

We would like to prove the converse of this statement. That is, our goal in the next couple of lectures is to prove the following result formulated by Fermat.

Theorem 7.4 (Fermat)**.** *A prime p can be written as the sum of two squares if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*

Proof. One of the direction is easy. Assume $p = a^2 + b^2$. Since a^2 and b^2 are each either congruent to 0 or 1 modulo 4, it follows that $p \equiv 0, 1$ or $2 \pmod 4$. But let's not forget that p is a prime, so it cannot possible be divisible by 4, and the only way it can be $\equiv 2 \pmod 4$ is for it to equal 2.

The other direction is much harder. It's clear to do when $p = 2$, but we also have to show that any prime $p \equiv 1 \pmod 4$ can be written as the sum of two squares. For that, we will follow Euler's proof. It might not be the shortest proof one can write down, but it has the advantage that it illustrates the concept of descent (which was the idea Fermat used in his sketch of the proof) and reciprocity that we will encounter again later in the course.

Reciprocity step: A prime $p \equiv 1 \pmod 4$, then it divides $N = a^2 + b^2$ with a and b relatively prime integers.

Descent step: If a prime p divides a number N of the form $N = a^2 + b^2$, where $(a, b) = 1$, then p itself can be written as $p = x^2 + y^2$ for some $(x, y) = 1$.

Clearly the these two claims imply our result. □

We are going to deviate from the historical order and prove first the reciprocity step. (Euler first found the proof for the descent step.)

7.3.1 Reciprocity step

The reciprocity step follows immediately from the following result.

Lemma 7.5. *The equation*

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

has solutions $\iff$ $p = 2$ *or* $p \equiv 1 \pmod 4$.

Proof. **If** $p = 2$, then $x = 1$ is a solution.

If $p \equiv 1 \pmod 4$, then $4 \mid p - 1 = \phi(p)$ and therefore there exists an integer a with $\operatorname{ord}_p a = 4$. This means that $a^4 \equiv 1 \pmod p$ and $a, a^2, a^3 \not\equiv 1 \pmod 4$. We have

$$a^4 - 1 = (a^2 - 1)(a^2 + 1) \equiv 0 \pmod{p}.$$

But $a^2 - 1 \not\equiv 0 \pmod p$, hence $a^2 \equiv -1 \pmod p$, and $x = a$ is a solution of our equation.

If $p \equiv 3 \pmod 4$, assume that $x = a$ is a solution, i.e. $a^2 \equiv -1 \pmod p$. Then $a^4 \equiv 1 \pmod p$, so $\operatorname{ord}_p a \mid 4$. But we also know that $\operatorname{ord}_p a \mid \phi(p) = p - 1$. Hence $\operatorname{ord}_p a \mid (p - 1, 4) = 2$, which means that $a^2 \equiv 1 \pmod p$. The upshot is that $1 \equiv -1 \pmod p$, so $p \mid 2$. The only way this will happen is for $p = 2$, and we reached a contradiction.

□

7.3.2 Descent step

Fermat's idea (which he used on a number of other occasions), formalized in this case by Euler in this case, is to show that if we have a solution to a diophantine equation, then we can find a "smaller" (in some sense) solution. Iterating this process means that we can find smaller and smaller positive integers. Hence the process needs to terminate at some point, or we reach a contradiction.

Lemma 7.6. *If N is an integer of the form $N = a^2+b^2$ for some $(a, b) = 1$ and $q = x^2+y^2$ is a* prime *divisor of N, then there exist relatively prime integers c and d such that $N/q = c^2+d^2$.*

Proof. First note that since q has no trivial divisors, x and y are forced to be relatively prime. We have

$$x^2N - a^2q = x^2(a^2 + b^2) - a^2(x^2 + y^2) = x^2b^2 - a^2y^2 = (xb - ay)(xb + ay).$$

Since $q \mid N$, it follows that $x^2N - a^2q \equiv 0 \pmod q$, and so

$$(xb - ay)(xb + ay) \equiv 0 \pmod{q}.$$

Since q is a prime, this can happen only if one of the factors is divisible by q. Since we can change the sign of a without affecting our theorem, we can assume that $q \mid xb - ay$, that is $xb - ay = dq$ for some integer d.

We would like to show that $x \mid a+dy$. Since $(x,y)=1$, this is equivalent to showing that $x \mid y(a+dy)$. But

$$y(a+dy) = ay + dy^2 = xb - dq + dy^2 = xb - d(x^2+y^2) + dy^2 = xb - dx^2$$

which is divisible by x. Thus $x \mid a+dy$, so there exist an integer c such that $a+dy = cx$. Therefore

$$cxy = (a+dy)y = xb - dx^2 = x(b-dx)$$

and so

$$cy + dx = b.$$

Next we see that

$$N = a^2+b^2 = (cx-dy)^2 + (cy+dx)^2 = (x^2+y^2)(c^2+d^2) = q(c^2+d^2).$$

Since $(a,b)=1$ it follows that $(c,d)=1$ and the proof is complete. □

And now for the actual descent step, assume that we have an odd prime p (and thus $p>2$) that divides a number M of the form $M=a^2+b^2$ with $(a,b)=1$. We want to show that $p \equiv 1 \pmod 4$.

First, note that we can add or subtract any multiple of p from a or b without changing the problem. That is, we can find integers a_1, b_1 with $|a_1|, |b_1| < p/2$ such that $p|N_1 = a_1^2+b_1^2$. In particular, $N_1 < p^2/2$. Denote $d = (a_1, b_1)$ Then $d < p/2$, so $p \nmid d$. We also know that $a_1 = da_2, b_1 = db_2$ and $(a_2, b_2) = 1$. Note that $|a_2| \le |a_1| < p/2$ and likewise $|b_2| < p/2$. Therefore $N_2 = a_2^2 + b_2^2 < p^2/2$.

We have

$$p \mid a_1^2 + b_1^2 = d^2(a_2^2+b_2^2).$$

Since p is a prime that does not divide d, it follows that $p|N_2 = a_2^2+b_2^2$.

So we showed that our prime p has to divide a number $M = u^2+v^2 < p^2/2$ with $(u,v)=1$ and $|u|, |v| < p/2$. The positive integer $m = M/p$ will have to be $m < p/2$.

Let q be a *prime* divisor of m. Clearly $q \neq p$ since $q \le m < p/2$. In particular $q < p$ and $p \mid \frac{M}{q}$.

Assume that q can be written as the sum of two squares. By Lemma 7.6, we have $M/q = x^2+y^2$ for some integers $(x,y)=1$. But then $p \mid x^2+y^2 < u^2+v^2 = M$.

So if all the prime factors of M different from p can be written as sums of two squares, then so can p. Since we assumed that this is not the case, it follows that M has some prime divisor $p_1 < p$ that cannot be written as the sum of two squares. By repeating the argument for p_1 it follows that there must exist another prime $p_2 < p_1$ that cannot be written as the sum of two squares. This argument cannot continue indefinitely, so at some point we are bound to hit the prime number $5 = 2^2+1^2$ which **can** obviously be written as the sum of two squares. The descent step is now proven and this completes the proof of Theorem 7.4.

Note that we implicitly used the fact that if $(x, y) = 1$ then $3 \nmid x^2 + y^2$. To see this, recall that for any integer x we have $x \equiv 0, 1$ or $-1 \pmod 3$, so $x^2 \equiv 0$ or $1 \pmod 3$. Since $(x, y) = 1$ we cannot have $x^2 \equiv y^2 \equiv 0 \pmod 3$, so $x^2 + y^2 \not\equiv 0 \pmod 3$.

7.4 Arithmetic

Not just the ring of Gaussian integer, but the field $\mathbb{Q}(i)$ is equipped with a norm map $N : \mathbb{Q}(i) \to \mathbb{Q}_{\geq 0}$ given by $N(x+iy) = x^2+y^2 = |x+iy|^2 = (x+iy)(x-iy) = (x+iy)\overline{(x+iy)}$.

Again we have $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Q}(i)$ and $N(\alpha) = 0 \iff \alpha = 0$.

Example 7.7. Does $3 - 4i$ divide $2 + i$? We can do the division by taking the ratio and rationalizing the denominator (i.e. multiply both top and bottom of the fraction by the complex conjugate of the denominator).

$$\frac{2+i}{3-4i} = \frac{(2+i)(3+4i)}{(3-4i)(3+4i)} = \frac{2+11i}{25} = \frac{2}{25} + i\frac{11}{25} \notin \mathbb{Z}[i] \implies 3 - 4i \nmid 2 + i.$$

Example 7.8. Does 18 divide $5 + 17i$?

$$\frac{5+17i}{18} = \frac{5}{18} + \frac{17}{18}i \notin \mathbb{Z}[i] \implies 18 \nmid 5 + 17i.$$

Lemma 7.9. *An integer $c \in \mathbb{Z}$ divides a gaussian integer $a + bi$ if and only if $c|a$ and $c|b$ in $\mathbb{Z}$.*

Proof.

$$c \mid a + bi \iff \frac{a+bi}{c} \in \mathbb{Z}[i] \iff \frac{a}{c} + \frac{b}{c}i \in \mathbb{Z}[i] \iff \frac{a}{c}, \frac{b}{c} \in \mathbb{Z} \iff c|a \text{ and } c|b.$$

□

Proposition 7.10. *If $\alpha, \beta \in \mathbb{Z}[i]$ and $\alpha \mid \beta$ in $\mathbb{Z}[i]$, then $N(\alpha) \mid N(\beta)$ as integers.*

Proof.

$$\alpha \mid \beta \implies \beta = \alpha\gamma \text{ for some } \gamma \in \mathbb{Z}[i] \implies N(\beta) = N(\alpha)N(\gamma) \implies N(\alpha) \mid N(\beta).$$

□

The converse is not true in general. For instance, $N(5)|N(3 - 4i)$ (both norms are equal to 25), but $5 \nmid 3 - 4i$.

There is however an exception. The element $1 + i$ has norm $N(1 + i) = 2$. We have the following result.

Proposition 7.11. *Let $\alpha = a + bi \in \mathbb{Z}[i]$. Then $N(1 + i) \mid N(\alpha)$ if and only if $(1 + i) \mid \alpha$.*

Proof. Clearly $(1+i) \mid \alpha$ implies $N(1+i) \mid N(\alpha)$. Conversely, we know that $2 \mid a^2+b^2$. We want to show that there exist $m, n \in \mathbb{Z}$ such that

$$a+bi = (1+i)(m+ni).$$

Expanding the right hand side we see that

$$a+bi = (1+i)(m+ni) \iff a = m-n, b = m+n.$$

We solve this 2×2 linear system in the unknowns m, n and find that $m = \frac{a+b}{2}$ and $n = \frac{b-a}{2}$. In order for these two numbers to be integers we need $a+b$ and $b-a$ to be even. But we know that $2 \mid a^2+b^2$, so a and b are either both even or both odd, i.e. $a \equiv b (\text{mod } 2)$. Hence $2 \mid a+b, b-a$ and the result is proved. □

Recall the long division in $\mathbb{Z}[i]$: for any $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$ there exist $\gamma, \rho \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma + \rho$ and $0 \leq N(\rho) < N(\beta)$.

However, as opposed to the division algorithm on $\mathbb{Z}$, we **do not** have uniqueness for γ and ρ. For instance, take $\alpha = -9, \beta = -5$. We have

$$-9 = (-5) \times 1 + (-4)$$

and

$$-9 = (-5) \times 2 + 1.$$

Both 1 and -4 have norm strictly smaller than the norm of -5. Indeed, $N(1) = 1 < 25 = N(-5)$ and $N(-4) = 16 < 25 = N(5)$.

Since $\mathbb{Z}[i]$ is an euclidean ring, it is also a unique factorization domain. But note that the factorization is unique up to multiplication by units. This was already the case over $\mathbb{Z}$. Namely, we know that "any nonzero integer n can be written as a product of primes". But what we really mean by this is that

$$n = (\pm 1)p_1 \dots p_r$$

with $p_1, \dots, p_r$ prime integers (and here is understood that they are positive). But in $\mathbb{Z}[i]$ there is no positivity, so for instance $1+i$ and $1-i$ really represent the same prime. That is, we see that they only differ by a unit, i.e.

$$\frac{1+i}{1-i} = \frac{(1+i)^2}{(1+i)(1-i)} = \frac{2i}{2} = i, \text{ so } (1+i) = i(1-i).$$

In particular, $1+i$ and $1-i$ generate the same ideal of $\mathbb{Z}[i]$. We will write $\pi_1 \sim \pi_2$ if they are two primes in $\mathbb{Z}[i]$ and there is a unit $\mu \in \mathbb{Z}[i]$ such that $\pi_1 = \mu\pi_2$. The unique factorization in $\mathbb{Z}[i]$ tells us that any nonzero gaussian integer α can be written as

$$\alpha = \mu\pi_1 \dots \pi_r$$

where $\mu \in U(\mathbb{Z}[i])$ and $\pi_1, \ldots, \pi_r$ are prime gaussian integers (not necessarily distinct. Moreover, if we have another factorization

$$\alpha = \nu\sigma_1 \ldots \sigma_s$$

then $r = s$ and for each $1 \leq j \leq r$ there exits $1 \leq k_j \leq r$ such that $\pi_j \sim \sigma_{k_j}$.

Definition. *Just like for regular integers, we say that two gaussian integers α, β are* relatively prime *if they have only unit factors in common.*

Definition. *For two elements $\alpha, \beta \in \mathbb{Z}[i]$,* a greatest common divisor *is a divisor of maximal norm.*

Note that this definition does not define a unique gaussian integer. If you have found a greatest common divisor δ of α, β then $\pm\delta, \pm i\delta$ (that is, δ multiplied by the units) are also divisors with maximal norm. But this is all the indeterminacy, since a greatest common divisor δ of two numbers with prime factorizations

$$\alpha = \mu_1\pi_1^{m_1} \ldots \pi_r^{m_r} \quad \beta = \mu_2\pi_1^{n_1} \ldots \pi_r^{n_r}$$

with $\pi_1, \ldots, \pi_r$ prime elements of $\mathbb{Z}[i]$, μ_1, μ_2 units, $m_j, n_j \geq 0$ is of the form

$$\delta = \mu\pi_1^{\min\{m_1,n_1\}} \ldots \pi_r^{\min\{m_r,n_r\}}$$

for some $\mu \in U(\mathbb{Z}[i])$.

Lemma 7.12. *(i) Assume that $\alpha \mid \beta\gamma$ are gaussian integers and that α, β are relatively prime. Then $\alpha \mid \gamma$.*

(ii) Assume that $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ such that $\alpha \mid \gamma$ and $\beta \mid \gamma$. If α and β are relatively prime, then $\alpha\beta \mid \gamma$.

Proof. Follows from unique factorization. □

Proposition 7.13. *If $\alpha, \beta \in \mathbb{Z}[i]$ and there exist $\gamma, \delta \in \mathbb{Z}[i]$ such that $\alpha\gamma + \beta\delta$ is a unit in $\mathbb{Z}[i]$, then α, β are relatively prime. In particular, if $a, b \in \mathbb{Z}$ are relatively prime integers, then they are also relatively prime in $\mathbb{Z}[i]$.*

Proof. If $\tau \in \mathbb{Z}[i]$ divides both α and β, then $\tau \mid (\alpha\gamma + \beta\delta)$, which is a unit. Therefore $N(\tau) \mid 1$. Thus $N(\tau) = 1$ and τ has to be a unit.

Since $a, b \in \mathbb{Z}$ are relatively prime, it follows that there exist $m, n \in \mathbb{Z}$ such that

$$am + bn = 1.$$

By the first part, they are relatively prime in $\mathbb{Z}[i]$. □

7.5 The prime elements of $\mathbb{Z}[i]$

Proposition 7.14. *If $\alpha \in \mathbb{Z}[i]$ has norm $N(\alpha) = p$ a prime integer, then α is a prime element of $\mathbb{Z}[i]$.*

Proof. Assume that $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathbb{Z}[i]$. Then $N(\beta)N(\gamma) = N(\alpha) = p$ is a prime number. Since $N(\beta), N(\gamma) \in \mathbb{Z}$, it follows that either $N(\beta) = 1$ or $N(\gamma) = 1$. By the previous lemma, this means that either β is a unit or γ is a unit. Hence α has no nontrivial divisors, and is therefore a prime gaussian integer. □

We want to find all elements $\pi = a + bi \in \mathbb{Z}[i]$ that are prime gaussian integers. We have seen in Proposition 7.14 that if the norm of a gaussian integer α is prime, then α is prime in $\mathbb{Z}[i]$. On the other hand, 3 is a prime in $\mathbb{Z}[i]$ but its norm $N(3) = 9$ is not a prime.

Lemma 7.15. *If $\pi \in \mathbb{Z}[i]$ is a prime element, then there exist a prime number $p \in \mathbb{Z}$ such that $\pi \mid p$ in $\mathbb{Z}[i]$.*

Proof. The norm $N(\pi)$ is a positive integer, and therefore it factors as a product of primes in $\mathbb{Z}$,

$$N(\pi) = p_1 \dots p_r.$$

On the other hand, $N(\pi) = \pi\bar{\pi}$, so $\pi \mid N(\pi)$. Thus

$$\pi \mid p_1 \dots p_r \implies \pi \mid p_j \text{ for some } 1 \leq j \leq r.$$

□

Theorem 7.16. *Let $p \in \mathbb{Z}$ be a (positive) prime. Its factorization in $\mathbb{Z}[i]$ is determined by its residue class modulo 4 as follows.*

(i) $2 = (1+i)(1-i) = -i(1+i)^2 = i(1-i)^2$ *and* $1+i = i(1-i)$ *represent the same prime ideal in* $\mathbb{Z}[i]$.

(ii) If $p \equiv 1 \pmod 4$ *then* $p = \pi\bar{\pi}$ *where* $\pi, \bar{\pi}$ *are two prime gaussian integers that are complex conjugates, but not unit multiples. In particular, they generate different prime ideals in* $\mathbb{Z}[i]$.

(iii) If $p \equiv 3 \pmod 4$ *then p is prime in* $\mathbb{Z}[i]$.

Proof. *(i)* Direct calculation.

(ii) If $p \equiv 1 \pmod 4$, Theorem 7.4 says that p can be written as a sum of two relatively prime squares $p = a^2 + b^2 = (a + bi)(a - bi)$. Set $\pi = a + bi$. Then $\bar{\pi} = a - bi$ and clearly $p = \pi\bar{\pi}$. Moreover $N(\pi) = N(\bar{\pi}) = a^2 + b^2 = p$ is prime, so π and $\bar{\pi}$ are prime gaussian integers by Proposition 7.14. Lastly,

$$\frac{a+bi}{a-bi} = \frac{(a+bi)^2}{a^2+b^2} = \frac{a^2-b^2}{a^2+b^2} + i\frac{2ab}{a^2+b^2} \notin \mathbb{Z}[i]$$

since both fractions have absolute value smaller than 1.

(*iii*) If $p \equiv 3 (\text{mod } 4)$, this follows from Proposition 7.2 and Theorem 7.4.

□

Lemma 7.15 tells us that any gaussian prime is a factor of a prime $p \in \mathbb{Z}$. Theorem 7.16 tells us how integral primes factor in $\mathbb{Z}[i]$. We put these two results together and get a complete characterization of the prime elements in $\mathbb{Z}[i]$.

Theorem 7.17. *Every prime gaussian integer is a unit multiple of one of the following primes:*

(i) $1 + i$;

(ii) π *or* $\bar{\pi}$ *where* $N(\pi) = p$ *is a prime integer* $p \equiv 1 (\text{mod } 4)$;

(iii) a prime p *in* $\mathbb{Z}$ *with* $p \equiv 3 (\text{mod } 4)$. *In this case* $N(p) = p^2$.

Note that in the first two cases the prime gaussian integers have nonzero real and imaginary parts, while in the third case we get $\pm p, \pm ip$ which have either the real or the imaginary part equal to 0. Moreover, the only prime gaussian integer of even norm is $1 + i$ (up to unit multiples). Therefore we see that if we have $\alpha \in \mathbb{Z}[i]$ and its prime factorization

$$\alpha = \mu \pi_1 \dots \pi_r$$

does not contain a prime multiple of $1 + i$, then $N(\alpha) = N(\pi_1) \dots N(\pi_r)$ is an odd integer. We find this way another proof of the fact that $N(\alpha)$ is even $\iff 1 + i \mid \alpha$.

7.6 Representing integers as sums of squares

We saw that a prime can be written as a sum of two squares essentially only one way, if at all (Theorem 7.21). We have seen that other integers though can be written as sums of two squares in multiple ways. For instance, $50 = 5^2 + 5^2 = 7^2 + 1^2$. We can use the arithmetic in $\mathbb{Z}[i]$ to *systematically* construct integers that are sums of two squares in more than one way. Take the factorizations of 5 and 10 in $\mathbb{Z}[i]$. We have

$$5 = (1 + 2i)(1 - 2i) \quad 10 = (1 + 3i)(1 - 3i).$$

Thus 50 factors in two ways

$$50 = 5 \cdot 10 = \big((1 + 2i)(1 + 3i)\big) \cdot \big((1 - 2i)(1 - 3i)\big) = \big((1 + 2i)(1 - 3i)\big) \cdot \big((1 - 2i)(1 + 3i)\big)$$

This becomes

$$50 = (-5 + 5i)(-5 - 5i) = (7 - i)(7 + i),$$

which gives

$$50 = 5^2 + 5^2 = 7^2 + 1^2.$$

Different representations of an integer as a sum of two squares in $\mathbb{Z}$ correspond to rearranging prime factors in $\mathbb{Z}[i]$. Here's another example. Consider the factorizations of 5 and 13. We have

$$5 = (1+2i)(1-2i) \quad 13 = (2+3i)(2-3i).$$

Therefore

$$65 = 5 \cdot 13 = \big((1+2i)(2+3i)\big) \cdot \big((1-2i)(2-3i)\big) = \big((1+2i)(2-3i)\big) \cdot \big((1-2i)(2+3i)\big)$$

which becomes

$$65 = (-4+7i)(-4-7i) = (8+i)(8-i).$$

The two factorizations yield two ways of writing 65 as a sum of squares:

$$65 = 4^2 + 7^2 = 8^2 + 1^2.$$

Let us find an integer which can be written as the sum of two squares in *three* different ways. Start with

$$5 = (1+2i)(1-2i) \quad 13 = (2+3i)(2-3i) \quad 17 = (1+4i)(1-4i).$$

Consider the following products

$$\alpha = (1+2i)(2+3i)(1+4i) \quad \beta = (1-2i)(2+3i)(1+4i) \quad \gamma = (1+2i)(2-3i)(1+4i).$$

Then

$$\alpha = -32 - 9i \quad \beta = 12 + 31i \quad \gamma = 4 + 33i$$

are gaussian integers with

$$N(\alpha) = N(\beta) = N(\gamma) = 5 \cdot 13 \cdot 17 = 1105.$$

Therefore

$$1105 = 32^2 + 9^2 = 12^2 + 31^2 = 4^2 + 33^2.$$

Using this method you can construct systematically and without having to guess integers that can be represented as sums of two squares in four, five, ..., twenty, ... ways.

Moreover, the arithmetic of $\mathbb{Z}[i]$ allows us to classify the integers that can be represented as sums of two squares.

Lemma 7.18. *(a) An integer n can be written as the sum of two squares if and only if n is the norm of some gaussian integer.*

(b) If $m, n \in \mathbb{Z}$ can be written as sums of two squares, then mn can also be written as the sum of two squares.

Proof. (a) $n = a^2 + b^2 \iff n = N(a+bi)$

(b) By part (a), we know that there exist $\alpha, \beta \in \mathbb{Z}[i]$ such that $n = N(\alpha)$ and $m = N(\beta)$. Then $mn = N(\alpha\beta)$ is also the sum of two squares.

□

Theorem 7.19. *An integer $n > 1$ is a sum of two squares exactly when any prime factor of n which is $\equiv 3 (\text{mod } 4)$ occurs with even multiplicity.*

Proof. First we show any integer $n > 1$ having even multiplicity at its prime factors which are $\equiv 3(\text{mod } 4)$ can be written as a sum of two squares. The prime $2 = 1^2 + 1^2$ and any prime $p \equiv 1(\text{mod } 4)$ can be written as the sum of two squares, by Theorem 7.4. On the other hand, $q^2 = q^2 + 0^2$ is trivially the sum of two squares, for any prime $q \equiv 3(\text{mod } 4)$. Since sums of two squares are closed under multiplication (part (b) of the Lemma), it follows that n can be written as the sum of two squares.

Now we treat the converse direction: any $n > 1$ which is a sum of two squares has even multiplicity at any prime factor which is $\equiv 3(\text{mod } 4)$. We argue by induction on n.
The fact is obviously true for $n = 2 = 1^2 + 1^2$.
Let $n \geq 3$ be a sum of two squares. We assume that in any sum of two squares $< n$ the prime factors that are $\equiv 3(\text{mod } 4)$ occur with even powers. (This is the induction hypothesis.)
If n has no prime factors congruent to 3 modulo 4, then we have nothing to prove and the result is obviously true.
In case $n = a^2 + b^2$ has some prime factor $p \equiv 3(\text{mod } 4)$, we get that

$$p \mid (a + bi)(a - bi).$$

On the other hand p is prime in $\mathbb{Z}[i]$, so $p \mid a + bi$ or $p \mid a - bi$. But in either case we can take complex conjugates and obtain that $p = \bar{p} \mid a - bi$ *and* $p = \bar{p} \mid a + bi$. Thus

$$p^2 \mid (a + bi)(a - bi) = n.$$

On the other hand, $p \mid a + bi$ implies that $p \mid a$ and $p \mid b$ (Lemma 7.9). Then we can write $a = pa_1, b = pb_1$ for some $a_1, b_1 \in \mathbb{Z}$. Thus

$$n = p^2(a_1^2 + b_1^2)$$

and $n_1 = a_1^2 + b_1^2 < n$. By the induction hypothesis, any prime $\equiv 3(\text{mod } 4)$ that appears in the factorization of n_1 appears with an even exponent. Therefore the same holds for n and our proof is complete.

□

Example 7.20. For primes we have seen that $p \equiv 1(\text{mod } 4) \implies p$ can be written as the sum of two squares. But the number $21 = 3 \cdot 7$ cannot be written as the sum of two squares, even though $21 \equiv 1(\text{mod } 4)$. In general, we need to factor an integer $n > 1$ in order to decide if it can be written as the sum of two squares.

7.7 More applications to the arithmetic of $\mathbb{Z}$

7.7.1 Primality testing: Fermat primes

Fermat conjectured that the numbers of the form $2^{2^n}+1$ are prime. Indeed,

- for $n=0: 2^1+1=3$ is prime;
- for $n=1: 2^2+1=5$ is prime;
- for $n=2: 2^3+1=17$ is prime.

The others get a bit too big for us to be able to tell at a glance that they are prime. But $2^8+1=257$ can be checked by hand without too much trouble that it is prime. Same for $2^{2^4}+1=4097$.

However

$$2^{2^5}=2^{32}+1=4294967297$$

is too big to check by hand easily. Note that $2^{32}+1=(2^{16})^2+1^2$ is the sum of two squares. Euler found that it has another very different representation as sum of two squares, namely

$$(2^{16})^2+1^2=4294967297=62264^2+20449^2.$$

The following theorem implies that the fifth Fermat number is in fact **not** a prime.

Theorem 7.21. *If p is a prime that can be written as sum of two squares, then it can be written like that in essentially one way. That is, if $p=a^2+b^2=c^2+d^2$, with $a,b,c,d,\in\mathbb{Z}$, then either $a=\pm c, b=\pm d$ or $a=\pm d, b=\pm c$.*

Proof. We have

$$(a+bi)(a-bi)=a^2+b^2=c^2+d^2=(c-di)(c+di)$$

and

$$N(a+bi)=N(a-bi)=a^2+b^2=p$$
$$N(c+di)=N(c-di)=c^2+d^2=p.$$

Since p is a prime, it follows from Proposition 7.14, that $a+bi, a-bi, c+di, c-di$ are all prime elements in $\mathbb{Z}[i]$. By the unique factorization, it follows that either $a+bi=\mu(c+di)$ for some $\mu\in U(\mathbb{Z}[i])$ or $a+bi=\mu(c-di)$ for some $\mu\in U(\mathbb{Z}[i])$.

If $a+bi=\mu(c+di)$ we have four possibilities.

- $\mu=1 \implies a=c, b=d$
- $\mu=-1 \implies a=-c, b=-d$
- $\mu=i \implies a=-d, b=c$
- $\mu=-i \implies a=d, b=-c$

The other case is similar. □

Note that the Theorem does not mention $\mathbb{Z}[i]$, it is a statement purely about integers. The proof however hinges on the arithmetic of the gaussian integers.

7.7.2 Pythagorean triples revisited

We start with the diophantine equation

$$a^2 + b^2 = c^2. \tag{7.1}$$

As before we reduce to the case where a, b, c are positive integers with $(a, b) = (b, c) = (c, a) = 1$, a odd and b even. Then c must also be odd.

Our equation (7.1) can be rewritten as

$$(a + bi)(a - bi) = c^2. \tag{7.2}$$

Claim 1 $a + bi$ and $a - bi$ are relatively prime.

Proof. Assume $\delta \mid a + bi$ and $\delta \mid a - bi$. Then $\delta \mid 2a$ and $\delta \mid 2bi \implies \delta \mid 2b$. If δ and $2 = -i(1 + i)^2$ were not relatively prime, then $1 + i \mid \delta \implies 2 \mid N(\delta)$. On the other hand, $\delta \mid c^2$, so $N(\delta) \mid c^4$ which is odd. This is a contradiction, so δ and 2 are relatively prime in $\mathbb{Z}[i]$. Then, Lemma 7.12 implies that

$$\delta \mid a, \delta \mid b.$$

But a, b are relatively prime, so δ must be a unit. □

Claim 2 There exist $\alpha, \beta \in \mathbb{Z}[i]$ such that either $a + bi = \alpha^2$ and $a - bi = \beta^2$ or $a + bi = i\alpha^2$ and $a - bi = -i\beta^2$.

Proof. Exercise. □

Since $a + bi$ and $a - bi$ are relatively prime, α, β are also relatively prime.

Thus $a + bi = \alpha^2 = (m + ni)^2$ or $a + bi = i\alpha^2 = i(m + ni)^2$ for some $m, n \in \mathbb{Z}$. Expanding the square leads to

$$a + bi = m^2 - n^2 + 2mni \quad \text{or} \quad a + bi = -2mn + i(m^2 - n^2).$$

However, we want a to be odd, so the second case cannot occur. We are therefore in the first case and $a + bi$ is after all a perfect square in the $\mathbb{Z}[i]$, i.e.

$$a + bi = (m + ni)^2 \text{ with } m, n \in \mathbb{Z}. \tag{7.3}$$

The derivation of (7.3) from unique factorization in $\mathbb{Z}[i]$ is the key step in this proof. The rest is a matter of (careful) book-keeping. Identifying the real and imaginary parts above gives

$$a = m^2 - n^2, b = 2mn$$

and therefore

$$c^2 = a^2+b^2 = (m^2-n^2)^2+(2mn)^2 = m^4+n^4-2m^2n^2+4m^2n^2 = m^4+n^4+2m^2n^2 = (m^2+n^2)^2.$$

Since $c > 0$ it follows that

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

We also have $b > 0$ so both m, n have to have the same sign, and by changing that sign we can assume without changing the values of a, b, c that $m, n > 0$. Since $a > 0$ we must have $m > n$. They also have to be relatively prime, since a, b are relatively prime. Lastly, since a is odd, $m \not\equiv n (\text{mod } 2)$.

We need to check that our solution $(a, b, c) = (m^2 - n^2, 2mn, m^2 + n^2)$ with $m > n > 0, (m, n) = 1, m \not\equiv n (\text{mod } 2)$, satisfies (7.1) and that a, b, c are positive integers with $(a, b) = (b, c) = (c, a) = 1$, a odd and b even. Indeed,

$$a^2 + b^2 = (m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2 = c^2.$$

On the other hand, $m \not\equiv n (\text{mod } 2) \implies a$ odd, and $b = 2mn$ is clearly even. Since $m > n > 0$ we have $a, b, c > 0$. If a prime p divides two of $m^2 - n^2, 2mn, m^2 + n^2$ then $p \neq 2$ since the first and third numbers are odd. Assume $p | m^2 - n^2$ and $p | 2mn$. Then $p | mn$ so $p | m$ or $p | n$. Assume $p | m$. Then $p | n^2$ and so $p | n$. This cannot happen since $(m, n) = 1$. The other case is similar.

To recap: we found a way of producing Pythagorean triples on demand. That is, take any gaussian integer α with both the real and imaginary parts non-zero, square it and get $\alpha^2 = a + bi$. Then $(|a|, |b|, N(\alpha))$ is a Pythagorean triple.

Example 7.22. $(23 + 10i)^2 = 529 - 100 + 460i = 429 + 460i$ and $23^2 + 10^2 = 629$. So $(429, 460, 629)$ is a Pythagorean triple. (Grab a calculator and check!) And since $(23, 10) = 1$ the triple is relatively prime.

7.7.3 Other diophantine equations

To better appreciate this approach to Pythagorean triples, let's apply it to the diophantine equation

$$a^2 + b^2 = c^3. \tag{7.4}$$

Theorem 7.23. *The integral solutions to*

$$a^2 + b^2 = c^3$$

with $(a, b) = 1$ *are given by the parametric formulas*

$$a = m^3 - 3mn^2, b = 3m^2n - n^3, c = m^2 + n^2, \text{ where } (m, n) = 1, m \not\equiv n \pmod 2.$$

Different choices of m, n *give different solutions* (a, b, c).

Proof. Note that a and b cannot both be even since they are relatively prime. On the other hand, if they were both odd we would have $a^2, b^2 \equiv 1 (\text{mod } 8)$ and therefore $c^3 \equiv 2 (\text{mod } 8)$

which is impossible. (In this case, c would have to be even, which would make c^3 a multiple of 8.) This $a \not\equiv b (\text{mod } 2)$ and c is odd. We can rewrite (7.4) as

$$c^3 = (a + bi)(a - bi). \tag{7.5}$$

We first show that $a + bi$ and $a - bi$ are relatively prime gaussian integers. Let $\delta \in \mathbb{Z}[i]$ such that $\delta \mid a + bi$ and $\delta \mid a - bi$. As we have seen in the previous section, this implies that

$$\delta \mid 2a, \delta \mid 2b.$$

On the other hand $N(\delta) \mid a^2 + b^2$ which is odd, so $N(\delta)$ is odd and thus δ and 2 are relatively prime. It follows that

$$\delta \mid a, \delta \mid b.$$

Since $(a, b) = 1$ it follows that δ is a unit in $\mathbb{Z}[i]$.
Hence $a + bi$ and $a - bi$ are relatively prime. From (7.5) follows that $a + bi = \mu\alpha^3$ for some $\mu \in U(\mathbb{Z}[i]), \alpha \in \mathbb{Z}[i]$. On the other hand, every unit in $\mathbb{Z}[i]$ is itself a cube:

$$1 = 1^3, -1 = (-1)^3, i = (-i)^3, -i - i^3.$$

Therefore we can write $\mu = \nu^3$ and so $a + bi = (\nu\alpha)^3$ and $\nu\alpha = \beta \in \mathbb{Z}[i]$. Thus

$$a + bi = (m + ni)^3 \text{ for some } m, n \in \mathbb{Z}.$$

Every prime $p \in \mathbb{Z}$ that divides both m and n would have to divide a and b. Therefore $(m, n) = 1$. We expand the cube and see that

$$a = m^3 - 3mn^2 \quad b = 3m^2n - n^3.$$

If $m \equiv n (\text{mod } 2)$, then we would get

$$a \equiv m^3 - 3m^3 \pmod 2 \equiv 0 \pmod 2$$

and

$$b \equiv 3m^3 - m^3 \pmod 2 \equiv 0 \pmod 2$$

which contradicts the fact that $a \not\equiv b (\text{mod } 2)$. Hence $m \not\equiv n (\text{mod } 2)$. Plugging the value of $a + bi = (m + ni)^3$ into (7.5) we see that

$$c^3 = (m + ni)^3(m - ni)^3 = (m^2 + n^2)^3 \implies c = m^2 + n^2.$$

We have to check two things. First, that our parametric equations give a solution (a, b, c) to (7.4) with $(a, b) = 1$ and $a + bi = (m + ni)^3$. Second, that changing the m, n changes the (a, b, c). The first is a direct calculation. The second uses the fact that the only cube root of unity in $\mathbb{Z}[i]$ is 1 itself. We know this since the norm of a cube root of 1 would have to be 1 and so the cube roots of unity are in $U(\mathbb{Z}[i])$. But we have seen what the cubes of the elements in $U(\mathbb{Z}[i])$ are from above. This means that if $(m + ni)^3 = (m' + n'i)^3$ we must have $m + ni = m + n'i$ hence $m = m'$ and $n = n'$.

□

Here's a table with a few solutions (a, b, c) to (7.4) for various choices of m and n.

m	n	$a = m^3 - 3mn^2$	$b = 3m^2n - n^3$	$c = m^2 + n^2$
1	0	1	0	1
2	1	2	11	5
3	2	-9	46	13
4	1	52	47	17
4	3	-44	9	25
7	2	259	286	53

Another application is to show that a perfect square in $\mathbb{Z}$ cannot come just before a perfect cube.

Theorem 7.24. *The only integers a, b satisfying $a^2 = b^3 - 1$ are $a = 0, b = 1$.*

On the face of it, this is not at all obvious. Besides, there are plenty of perfect cubes that come just before a perfect square: -1 and 0; 0 and 1; 8 and 9.

Proof. Clearly $a = 0, b = 1$ satisfy $a^2 = b^3 - 1$. We want to show that there are no other solutions. Assume $a, b \in \mathbb{Z}$ do satisfy

$$a^2 = b^3 - 1.$$

We can rewrite this equation as

$$b^3 = (a - i)(a + i)$$

and follow the blueprint from the previous theorem. If we know that $a + i$ and $a - i$ are relatively prime, then, recalling that the only cube root of unity is 1 itself, we see that $a + i$ and $a - i$ have to be perfect cubes in $\mathbb{Z}[i]$ and we would get

$$a = m^3 - 3mn^2, 1 = 3m^2n - n^3$$

for some $m, n \in \mathbb{Z}$. The second relation shows that $n \mid 1$, so $n = \pm 1$. If $n = 1$, we have $1 = 3m^2 - 1$ so $3m^2 = 2$ which is impossible. Thus $n = -1$ and therefore $1 = 1 - 3m^2$ so $m = 0$. This leads us to $a = 0$ and $b^3 = 1$, so $b = 1$.

It remains to show that $a + i$ and $a - i$ are relatively prime gaussian integers. Assume δ is a common divisor. Then $\delta | 2a$ and $\delta \mid 2i = (1 + i)^2$. Thus, up to units, δ is either 1 or $1 + i$ or $(1 + i)^2$. Assume δ is not a unit. Then $(1 + i) \mid \delta$ and therefore $(1 + i) \mid b^3$. Since $1 + i$ is a prime gaussian integer, we then have $(1 + i) \mid b$, hence $b^2 = N(b)$ is even. Thus b must be even, and therefore $a \equiv -1 (\text{mod } 4)$ which is impossible. □

Remark 7.25. In 1850, Lebesgue used $\mathbb{Z}[i]$ to show that, for $d \geq 2$, the only integral solution to

$$y^2 = x^d - 1$$

is $x = 1, y = 0$.

8 Diophantine equations and congruences

As we have already seen in some isolated examples, one can try to show that a diophantine equation does not have solutions by showing that it has no solution modulo some integer n.

Example 1 $x^2 - 3y^2 = -1$

Looking at this equation modulo 3, we see that

$$x^2 \equiv -1 \pmod 3,$$

which we know it is impossible since $3 \nmid 1$.

Example 2 $x^2 - 7y^2 = -1$

This implies that $x^2 + 1 \equiv 0 \pmod 7$ and that is impossible since 7 is a prime and $7 \equiv 3 \pmod 4$.

Example 3 $x^2 - 15y^2 = 2$

This implies that $x^2 \equiv 2 \pmod 5$. But the only squares modulo 5 are $0, 1, 4$.

Example 4 $x^2 - 5y^2 = 3z^2$

Assume that we have a positive solution with $(x, y, z) = d$. Then $x = dx_1, y = dy_1, z = dz_1$ with $(x_1, y_1, z_1) = 1$ and

$$x_1^2 - 5y_1^2 = 3z_1^2.$$

In particular, $3 \mid x_1^2 - 5y_1^2$ and, since obviously $3 \mid 6y_1^2$, we get $3 \mid x_1^2 + y_1^2$. We know that this is only possible if $3 \mid x_1$ and $3 \mid y_1$. But then $9 \mid 3z_1^2$ and so $3 \mid z_1$. This cannot happen since $(x_1, y_1, z_1) = 1$.

9 Quadratic rings

We begin by looking at the ring $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d}\,; a, b \in \mathbb{Z}\}$ for some $d \in \mathbb{Z}$. The ring $\mathbb{Z}[\sqrt{d}]$ is clearly contained in the field $\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d}\,; x, y \in \mathbb{Q}\}$.

Exercise 9.1. Prove that $\mathbb{Z}[\sqrt{d}]$ is a ring, that $\mathbb{Q}(\sqrt{d})$ is a field. Show that if d is a perfect square, then $\mathbb{Z}[\sqrt{d}] = \mathbb{Z}$ and $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$. Furthermore, if $d = d_1 d_2^2$ then $\mathbb{Z}[\sqrt{d}] = \mathbb{Z}[\sqrt{d_1}]$ and $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d_1})$.

Lemma 9.2. *The map $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{R}$ given by $N(x + y\sqrt{d}) = x^2 - dy^2$ is multiplicative (i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$) and*

$$N(\alpha) = 0 \iff \alpha = 0.$$

Note that this map does not necessarily make $\mathbb{Z}[\sqrt{d}]$ into an Euclidean ring. To begin with, it could take negative values, e.g. $N(1+\sqrt{6}) = -5$ in $\mathbb{Z}[\sqrt{6}]$. In fact, whenever $d > 1$ the map N will take negative values. When $d < 0$, the map N takes only nonnegative values. But even then, $\mathbb{Z}[\sqrt{d}]$ could fail to be an Euclidean ring. For instance, $\mathbb{Z}[\sqrt{-6}] = \mathbb{Z}[i\sqrt{6}]$ is not an UFD ($6 = -\sqrt{-6} \cdot \sqrt{-6} = 2 \cdot 3$.) and therefore not an Euclidean ring.

Proposition 9.3. *An element $\alpha \in \mathbb{Z}[\sqrt{d}]$ is a unit in the ring $\mathbb{Z}[\sqrt{d}]$ if and only if $N(\alpha) = \pm 1$.*

Proof. Assume α is a unit. Then there exist $\beta \in \mathbb{Z}[\sqrt{d}]$ such that $\alpha\beta = 1$. Therefore $N(\alpha)N(\beta) = 1$. Since $N(\alpha)$ and $N(\beta)$ are integers, the only way this can happen is if $N(\alpha) = N(\beta) = \pm 1$.

Conversely, assume $N(\alpha) = \pm 1$. On the other hand $\alpha = a + b\sqrt{d}$, so $N(\alpha) = \alpha(a - b\sqrt{d})$. Then $\beta = \pm(a - b\sqrt{d})$ is the inverse of α in $\mathbb{Z}[\sqrt{d}]$. □

9.1 Units in imaginary quadratic rings

An imaginary quadratic ring is of the form $\mathbb{Z}[\sqrt{d}]$ with $d < 0$. For instance the gaussian integers $\mathbb{Z}[i]$ are such a ring ($d = -1$). If $d < 0$ then the norm map $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{R}$ given by $N(x + y\sqrt{d}) = x^2 - dy^2$ takes only non-negative values. Therefore Proposition 9.3 says that $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ is a unit $\iff N(\alpha) = 1 \iff a^2 - db^2 = 1$. If $d = -1$ we have seen that this amounts to $\alpha = \pm 1, \pm i$. If $d < -1$, then the only way to have $a^2 - db^2 = 1$ is for $b = 0$ and $a = \pm 1$. Therefore we have the following result.

Theorem 9.4. *In an imaginary quadratic ring $\mathbb{Z}[\sqrt{d}]$ with $d < 0$, the units are*

$$U\left(\mathbb{Z}[\sqrt{d}]\right) = \begin{cases} \{\pm 1, \pm i\} & \text{if } d = -1 \text{ (gaussian integers)}; \\ \\ \{\pm 1\} & \text{if } d < -1. \end{cases}$$

9.2 Units in real quadratic rings: Fermat-Pell equations

Assume d is a positive integer. Then Proposition 9.3 says that the units in the real quadratic ring $\mathbb{Z}[\sqrt{d}]$ are exactly those elements $a + b\sqrt{d}$ with (a, b) satisfying one of the equations

$$x^2 - dy^2 = 1 \tag{9.1}$$

or

$$x^2 - dy^2 = -1. \tag{9.2}$$

So in order to determine the units in $\mathbb{Z}[\sqrt{d}]$ we need to solve these diophantine equations called Fermat-Pell equations. That is, we want to figure out for which d they have (non-trivial) integer solutions. (Trivial solutions are the ones where either $x = 0$ or $y = 0$.) If the answer is affirmative, we want to find a way to write down *all* solutions.

First a few examples.

Example 1 $x^2 - 3y^2 = -1$

Looking at this equation modulo 3, we see that

$$x^2 \equiv -1 \pmod 3,$$

which we know it is impossible since $3 \nmid 1$.

Example 2 $x^2 - 3y^2 = 1$

For instance $(2, 1)$ is a solution. In fact, it has infinitely many solutions as we shall see shortly.

Example 3 $x^2 - 7y^2 = -1$

This implies that $x^2 + 1 \equiv 0 \pmod 7$ and that is impossible since 7 is a prime and $7 \equiv 3 \pmod 4$.

Example 4 $x^2 - py^2 = -1$

has no solutions when p is a prime $p \equiv 3 \pmod 4$. The argument is the same as in the previous example.

We start our systematic study by proving the following result.

Theorem 9.5. *Let d be a positive integer.*

1. *If the equation*
$$x^2 - dy^2 = 1 \tag{9.1}$$
has one positive solution, then it has infinitely many positive solutions.

2. *If the equation*
$$x^2 - dy^2 = -1 \tag{9.2}$$
has one positive solution, then both (9.1) *and* (9.2) *have infinitely many positive solutions.*

The theorem follows immediately from the following lemma.

Lemma 9.6. *Assume that $a, b, d \in \mathbb{Z}_{>0}$ and let*

$$c = a^2 - db^2.$$

Then for any $n \geq 1$ there exist positive integers x_n, y_n such that

$$x_n^2 - dy_n^2 = c^n.$$

Moreover, we can choose these integers such that $\{x_n\}_n$ and $\{y_n\}_n$ are two strictly increasing sequences.

Proof. By induction on n. First, we have to check for $n = 1$. This is resolved by taking $x_1 = a$ and $y_1 = b$.

Now assume that we found x_n, y_n. Then

$$c^{n+1} = c^n \cdot c = (x_n^2 - dy_n^2)(a^2 - db^2) = a^2x_n^2 + d^2b^2y_n^2 - d(a^2y_n^2 + b^2x_n^2) = (ax_n + dby_n)^2 - d(ay_n + bx_n)^2.$$

Then

$$\begin{cases} x_{n+1} = ax_n + dby_n \\ y_{n+1} = ay_n + bx_n \end{cases}$$

have the property that

$$x_{n+1}^2 - dy_{n+1}^2 = c^{n+1}.$$

It remains to verify that $x_{n+1} > x_n$ and $y_{n+1} > y_n$. This is so because

$$x_{n+1} = ax_n + dby_n > ax_n \geq x_n$$

and

$$y_{n+1} = ay_n + bx_n > ay_n \geq y_n.$$

They are of course positive because $x_n > x_1 = a > 0$ and $y_n > y_1 = b > 0$ for all $n > 1$. □

Even though we proved that if a solution exists, then infinitely many solutions exits, we are far from done. We still have to figure out exactly when the Pell equations have solutions and how to generate all solutions.

For the rest of this section we assume that $d > 0$ is square-free.

9.3 Continued fractions

We still want a method for finding that smallest solution to Pell's equation (9.1). The answer will be provided in terms of continued fractions (and dates back to the dawn of time, or at least to VI century India).

Given a real number α one computes its continued fraction expansion as follows.

$$\begin{aligned} &\alpha_0 = \alpha, \qquad a_0 = \lfloor \alpha_0 \rfloor \quad \lambda_1 = \alpha_0 - a_0 \\ &\alpha_i = \frac{1}{\lambda_i}, \qquad a_i = \lfloor \alpha_i \rfloor \quad \lambda_{i+1} = \alpha_i - a_i \ \forall i \geq 1 \end{aligned} \tag{9.3}$$

The process stops if $\lambda_n = 0 \iff \alpha_n \in \mathbb{Z}$ for some n. This formula ensures that $\alpha_i, a_i \geq 1$ for all $i \geq 1$.

Definition. *We say that*

$$[a_0, a_1, \ldots] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}}$$

is the continued fraction of the real number α, where the a_i's are computed according to the procedure given in (9.3).

Example 9.7.

$$A = \frac{5}{3} = 1 + \frac{2}{3} = 1 + \frac{1}{\frac{3}{2}} = 1 + \frac{1}{1 + \frac{1}{2}}$$

The continued fraction expansion of $\frac{5}{3}$ is $[1, 1, 2]$.

Example 9.8. A finite continued fraction $[a_0, a_1, \ldots, a_n]$ with $a_i \geq 1$ for all $1 \leq i \leq n$, is a rational number. Vice versa, if $\frac{a}{b}$ is a rational number, the procedure (9.3) outlines the Euclidean algorithm for a and b. Thus the rational fraction of a rational number is finite, unique, and $\frac{a}{b}$ is equal to to its continued fraction.

Example 9.9. The continued fraction of $\sqrt{5}$ is $[2, 4, 4, 4, 4, \ldots]$.

Other examples

- $\sqrt[3]{2} = [1, 3, 1, 5, 1, 1, 4, 1, 1, 8, 1, 14, 1, 10, 2, 1, \ldots]$
- $\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, \ldots]$
- $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \ldots]$

Definition. *Let $[a_0, a_1, \ldots]$ be a continued fraction. The rational number*

$$s_n = \frac{p_n}{q_n} = [a_0, \ldots, a_n] \quad (n \geq 0)$$

is called the nth convergent *of* $[a_0, a_1, \ldots]$.

Example 9.10.

$$n = 0: \qquad s_0 = \frac{p_0}{q_0} = [a_0] = a_0 \qquad \Longrightarrow \quad p_0 = a_0, \qquad q_0 = 1$$

$$n = 1: \qquad s_1 = \frac{p_1}{q_1} = [a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} \quad \Longrightarrow \quad p_1 = a_0 a_1 + 1, \quad q_1 = a_1$$

We can continue this procedure and see that in general

$$\begin{aligned} p_{n+1} &= a_{n+1}p_n + p_{n-1} \quad \text{for all } n \geq 1, \quad p_0 = a_0, \qquad p_1 = a_0a_1 + 1; \\ q_{n+1} &= a_{n+1}q_n + q_{n-1} \quad \text{for all } n \geq 1, \quad q_0 = 1, \qquad q_1 = a_1. \end{aligned} \tag{9.4}$$

Note that

$$p_1q_0 - p_0q_1 = a_0a_1 + 1 - a_0a_1 = 1.$$

Furthermore, (9.4) implies that

$$p_{n+1}q_n - p_nq_{n+1} = (a_{n+1}p_n + p_{n-1})\, q_n - p_n\,(a_{n+1}q_n + q_{n-1}) = p_{n-1}q_n - p_nq_{n-1}.$$

It follows by induction that

$$p_{n+1}q_n - p_nq_{n+1} = (-1)^n \quad \forall n \geq 0. \tag{9.5}$$

In particular, p_n, q_n are relatively prime for all n and therefore the convergents $\dfrac{p_n}{q_n}$ are indeed written in lowest terms with p_n, q_n computed using the recurrence relations (9.4).

Moreover, if $[a_0, a_1, \ldots]$ is an infinite continued fraction (9.4) implies that the denominators q_n keep growing, while (9.5) tells us that $\dfrac{p_n}{q_n} - \dfrac{p_{n+1}}{q_{n+1}} = \dfrac{(-1)^n}{q_nq_{n+1}}$. Therefore the convergents $\dfrac{p_n}{q_n}, n \geq 0$, form a Cauchy sequence. We can now make the following definition.

Definition. *When we write $\alpha = [a_0, a_1, \ldots]$, we mean that $\alpha = \lim\limits_{n\to\infty} \dfrac{p_n}{q_n}$.*

Theorem 9.11. *If $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, then the continued fraction expansion of α is infinite and α is indeed equal to its continued fraction obtained according to* (9.3)*, i.e.*

$$\alpha = \lim_{n\to\infty} s_n = \lim_{n\to\infty} \frac{p_n}{q_n} = [a_0, a_1, \ldots].$$

Proof. Exercise. □

The above recurrence can be better understood in terms of *linear fractional transformations*.

9.3.1 Linear fractional transformations

Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a 2×2 matrix with complex coefficients. Recall that

$$\det M = ad - bc \quad M^t = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

and M has an inverse when $\det M \neq 0$. In this case,

$$M^{-1} = \frac{1}{\det M} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Each such matrix defines a function $\mathbb{C} \to \mathbb{C}$ given by

$$M(z) = \frac{az+b}{cz+d}.$$

Note that $M_1(M_2(z)) = (M_1 \cdot M_2)(z)$ and $I(z) = z$. (Exercise!)

Exercise 9.12. For each $n \geq 0$ let

$$M_n = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & a_0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & a_1 \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & a_n \end{bmatrix}.$$

Then

$$M_n = \begin{bmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{bmatrix}$$

and $s_n = M_n(0)$ and $\alpha = M_n(\lambda_{n+1})$.

Exercise 9.13. $s_0 < s_2 < s_4 < \ldots < s_{2n} < \ldots < \alpha < \ldots < s_{2n+1} < \ldots < s_5 < s_3 < s_1$ and $\lim_{n\to\infty} s_{2n} = \lim_{n\to\infty} s_{2n+1} = \lim_{n\to\infty} s_n = \alpha$.

Remark 9.14. We can also see immediately that $\det M_n = (-1)^{n+2} = (-1)^n$ as it is the product of $n+2$ matrices each with determinant (-1). This gives us a new proof of the fact that

$$p_{n-1}q_n - p_n q_{n-1} = (-1)^n.$$

(They are both equal to $\det M_n$.)

9.3.2 Best rational approximation

For any irrational number *alpha*, we have seen that the continued fraction algorithm produces a sequence of rational numbers $s_n = p_n/q_n$ which converges to α. We want to prove that these rational numbers are best approximations, in the following sense.

Theorem 9.15. *Let α be a positive irrational number and $n \geq 0$. Suppose that for some positive integers x, y we have*

$$\left|\frac{x}{y} - \alpha\right| < \left|\frac{p_n}{q_n} - \alpha\right|,$$

then $y > q_n$.

Proof. **Claim** $|s_n - \alpha| < |s_{n-1} - \alpha|$ (i.e. α is closer to s_n than to s_{n-1}. The claim follows if we show that the real number

$$r = \frac{\alpha - s_n}{\alpha - s_{n-1}}$$

has absolute value $|r| < 1$. To see this, let us examine

$$\frac{q_n}{q_{n-1}} \cdot r = \frac{q_n}{q_{n-1}} \cdot \frac{\alpha - p_n/q_n}{\alpha - p_{n-1}/q_{n-1}} = \frac{q_n\alpha - p_n}{q_{n-1}\alpha - p_{n-1}}.$$

Therefore

$$-\frac{q_n}{q_{n-1}} \cdot r = \frac{q_n\alpha - p_n}{-q_{n-1}\alpha + p_{n-1}} = A(\alpha)$$

where

$$A = \begin{bmatrix} q_n & -p_n \\ -q_{n-1} & p_n \end{bmatrix} = (\det M_n)M_n^{-1} = (-1)^n M_n^{-1}.$$

Hence

$$(-1)^{n+1}\frac{q_n}{q_{n-1}} \cdot r = M_n^{-1}(\alpha).$$

On the other hand, $\alpha = M_n(\lambda_{n+1}$ (cf. Exercise 9.12), so

$$(-1)^{n+1}\frac{q_n}{q_{n-1}} \cdot r = \lambda_{n+1}.$$

We have obtained the relation

$$r = (-1)^{n+1}\frac{q_{n-1}}{q_n} \cdot \lambda_{n+1},$$

so

$$|r| = \left|\frac{q_{n-1}}{q_n}\right| |\lambda_{n+1}| \leq |\lambda_{n+1}| < 1$$

as $q_n > q_{n-1}$ and $0 < \lambda_{n+1} < 1$. (Since α is irrational, $\lambda_{n+1} \neq 0$.) The claim is therefore proved.

Going back to the proof of the theorem, let I be the interval between s_n and s_{n-1}. Its length is

$$|s_n - s_{n-1}| = \left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{|\det M_n|}{q_n q_{n-1}} = \frac{1}{q_n q_{n-1}}.$$

We know that $\alpha \in I$, and by the above claim, we also know that α is closer to s_n than to s_{n-1}. Hence

$$\left|\frac{x}{y} - \alpha\right| < \left|\frac{p_n}{q_n} - \alpha\right| < \left|\frac{p_{n-1}}{q_{n-1}} - \alpha\right|$$

It follows that $\frac{x}{y} \in I$ and thus

$$\left|\frac{x}{y} - s_{n-1}\right| < \text{length}(I) = \frac{1}{q_n q_{n-1}}.$$

Therefore

$$\frac{1}{q_n q_{n-1}} > \left|\frac{x}{y} - s_{n-1}\right| = \left|\frac{x}{y} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{|xq_{n-1} - yp_{n-1}|}{yq_{n-1}} \tag{9.6}$$

Since I is an open interval, we have $\frac{x}{y} \neq s_{n-1}$ and therefore the numerator in (9.6) is a non-zero integer. It follows that the absolute value of said numerator is an integer ≥ 1. Thus, (9.6) implies that

$$\frac{1}{q_n q_{n-1}} > \frac{1}{yq_{n-1}} \implies y > q_n.$$

□

There is another, more visual way in which the numbers $s_n = p_n/q_n$ are best approximations. Consider the points (p, q) in the xy-plane, where p, q are positive integers. We call these *lattice points*. Each lattice point (p, q) determines a rational number p/q. Now draw the line L with equation $y = \alpha x$. Since α is irrational, this line L misses all the lattice points (p, q). Start your car at the origin $(0, 0)$, and travel up the line L, observing nearby lattice points as they pass by. Every time you see a lattice point (p, q) that gets closer to you than any previously seen lattice point, write down the rational number p/q. The remarkable fact is that the list you make will be none other than

$$s_1 = \frac{p_1}{q_1}, s_2 = \frac{p_2}{q_2}, s_3 = \frac{p_3}{q_3} \dots$$

So you can compute the best rational approximations to α without ever getting out of your car.

9.3.3 Continued fractions and quadratic numbers

Definition. *We say that a continued fraction is purely periodic if it is of the form*

$$[\overline{b_0, b_1, \dots, b_m}] = [b_0, b_1, \dots, b_m, b_0, b_1, \dots, b_m, b_0, b_1, \dots].$$

We say that a continued fraction is periodic if it is of the form

$$[a_0, \dots, a_k, \overline{b_0, b_1, \dots, b_m}] = [a_0, \dots, a_k, b_0, b_1, \dots, b_m, b_0, b_1, \dots, b_m, b_0, b_1, \dots].$$

Example 9.16. Let $\alpha = [a, \bar{b}]$. Note that our procedure (9.3) ensures that $b \geq 1$. Then

$$\alpha = a + \frac{1}{\beta}, \text{ where } \beta = [\,\bar{b}\,] > 1.$$

On the other hand,

$$\beta = b + \frac{1}{\beta},$$

so

$$\beta^2 = b\beta + 1.$$

Since $\beta > 0$, the quadratic formula tells us that

$$\beta = \frac{b + \sqrt{b^2+4}}{2},$$

and therefore

$$\alpha = a + \frac{2}{b+\sqrt{b^2+4}} \cdot \frac{-b+\sqrt{b^2+4}}{-b+\sqrt{b^2+4}} = \frac{2a - b + \sqrt{b^2+4}}{2}.$$

In particular, if $b = 2a$ we get that

$$[a, 2a, 2a, \ldots, 2a, \ldots] = \sqrt{a^2+1}.$$

We have already seen this for $a = 2$, namely we have seen that $\sqrt{5} = [2, \overline{4}]$.

Lemma 9.17. *If $\beta = [\overline{b_1, \ldots, b_m}]$ has a purely periodic continued fraction with, then there are positive integers x, y, u, v such that*

$$\beta = \frac{x\beta + y}{u\beta + v}.$$

Proof. The key observation here is, as above, that

$$\beta = b_1 + \cfrac{1}{\ddots + \frac{1}{b_m + \frac{1}{\beta}}}.$$

The rest is just algebraic manipulation. □

We can see that quadratic irrationals arise in the theory of continued fractions also using the fractional linear transformation approach. Suppose $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ is fixed by the integer matrix

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

That is, suppose we have

$$\frac{a\alpha + b}{c\alpha + d} = \alpha.$$

This amounts to the quadratic equation

$$c\alpha^2 - (a-d)\alpha - b = 0.$$

Since α is assumed to be irrational, we must have $c \neq 0$, so α is a quadratic irrational.

Before we proceed further, one more observation about continued fraction expansion via matrices. For any irrational number $\alpha = [a_0, a_1, \ldots]$ (not necessarily quadratic), the nth stage continued fraction expansion is of the form

$$\alpha = [a_0, \ldots, a_n, \alpha_{n+1}]$$

where

$$\alpha_{n+1} = [a_{n+1}, a_{n+2}, \dots].$$

In terms of matrices this means that

$$\alpha = M_n\left(\frac{1}{\alpha_{n+1}}\right) = \begin{bmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} (\alpha_{n+1}) = \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} (\alpha_{n+1}) \tag{9.7}$$

Remark 9.18. If it happens that $\alpha_{n+1} = \alpha$ for some n, then we have

$$\alpha = \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} (\alpha),$$

so α is a quadratic irrational and it satisfies the quadratic equation

$$q_n x^2 - (p_n - q_{n-1})x - p_{n-1} = 0. \tag{9.8}$$

Remark 9.19. If $\alpha = [a_0, \dots, a_k, \overline{b_0, b_1, \dots, b_m}]$ has a periodic continued fraction, then

$$\alpha = M_k(\alpha_{k+1}) = \begin{bmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{bmatrix} (\alpha_{k+1})$$

and $\alpha_{k+1} = [\overline{b_0, b_1, \dots, b_m}]$ is purely periodic.

Theorem 9.20. *(i) If the continued fraction expansion of a real number α is (eventually) periodic, i.e.*

$$\alpha = [a_0, \dots, a_k, \overline{b_0, b_1, \dots, b_m}],$$

then there exists $d \in \mathbb{Z}_{>0}$ not a square such that $\alpha \in \mathbb{Q}(\sqrt{d})$, but $\alpha \notin \mathbb{Q}$. Equivalently we can say that there exist integers r, s, t, d with $d > 0$ not a square, $s, t \neq 0$ such that

$$\alpha = \frac{r + s\sqrt{d}}{t}.$$

(ii) Let d be a positive integer that is not a perfect square and $r, s, t \in \mathbb{Z}$, $s, t \neq 0$. Then the continued fraction of

$$\alpha = \frac{r + s\sqrt{d}}{t}$$

is periodic. That is, the continued fraction of any irrational number in $\mathbb{Q}(\sqrt{d})$ is (eventually) periodic.

Proof. (i) Denote $\beta = [\overline{b_0, b_1, \dots, b_m}]$. Lemma 9.17 implies that β satisfies a quadratic equation

$$a\beta^2 + b\beta + c = 0.$$

Note that the discriminant $\Delta = b^2 - 4ac > 0$ since $\beta \in \mathbb{R} \setminus \mathbb{Q}$. (This is because β is the limit of a sequence of positive rational numbers, but it cannot be rational itself since its continued fraction is infinite.) In other words, β is of the form

$$\beta = \frac{r' + s'\sqrt{d}}{t'}$$

for some integers r', s', t'. In particular $\beta \in \mathbb{Q}(\sqrt{d})$ and since $\mathbb{Q}(\sqrt{d})$ is closed under addition, division and multiplication, it follows that $\alpha \in \mathbb{Q}(\sqrt{d}) \setminus \mathbb{Q}$ so α is of the desired form.

(*ii*) The argument for the second part is more complicated. The strategy will be as follows. Recall the procedure (9.3) for computing the continued fraction of α. The statement (*ii*) is equivalent to showing that there exist positive integers m, k such that $\alpha_k = \alpha_{k+m}$. (In this case, the continued fraction procedure ensures that $a_k = a_{m+k}$ and $\alpha_{k+1} = \alpha_{m+k+1}$, etc...) Note that it is enough to show that the set $\{\alpha_n; n \geq 0\}$ is finite. □

Definition. *The* discriminant *of a quadratic polynomial* $f(X) = aX^2 + bX + c$ *is*

$$\Delta(f) = b^2 - 4ac.$$

Definition. *Given a matrix* $M = \begin{bmatrix} u & v \\ y & z \end{bmatrix}$ *with nonzero determinant and a quadratic polynomial* $f(X) = aX^2 + bX + c$*, we associate to* f *and* M *another quadratic polynomial is*

$$f_M(X) = (yX + z)^2 f\left(\frac{uX + v}{yX + z}\right).$$

Note that $f_M(X) = \tilde{a}X^2 + \tilde{b}X + \tilde{c}$ where

$$\begin{aligned} \tilde{a} &= au^2 + buy + cy^2 = y^2 f\left(\frac{u}{y}\right) \\ \tilde{b} &= 2auv + b(uz + yv) + 2cyz \\ \tilde{c} &= av^2 + bvz + cz^2 = z^2 f\left(\frac{v}{z}\right). \end{aligned} \tag{9.9}$$

While the coefficients of f_M and f are quite different, their discriminants are related by

$$\Delta(f_M) = (\det M)^2 \Delta(f). \tag{9.10}$$

In particular, if $\det(M) = \pm 1$, then $\Delta(f_M) = \Delta(f)$.

We now go back to the proof of the Theorem 9.20.

Proof of (*ii*) *continued.* Recall that we want to show that the set $\{\alpha_n; n \geq 0\}$ is finite. In order to achieve this, we will actually show that all α_n's have to be among the roots of a

finite set of quadratic polynomials.

We start with the observation that if $\alpha \in \mathbb{Q}(\sqrt{d})$, then it is a root of some quadratic polynomial $f(X) = aX^2 + bX + c$. Since α is irrational, we can fix f definitively by requiring that a, b, c are relatively prime integers and $a > 0$. By (9.7), we know that

$$\alpha = \tilde{M}_n(\alpha_{n+1})$$

where

$$\tilde{M}_n = \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix}.$$

Thus we have

$$0 = f(\alpha) = f(\tilde{M}_n(\alpha_{n+1})) \implies 0 = f_{\tilde{M}_n}(\alpha_{n+1}).$$

On the other hand, we know that

$$f_{\tilde{M}_n}(X) = \tilde{a}_n X^2 + \tilde{b}_n X + \tilde{c}_n$$

where the coefficients $\tilde{a}_n, \tilde{b}_n, \tilde{c}_n$ are given by (9.9). It is important to note that

$$\tilde{c}_n = q_{n-1}^2 f\left(\frac{p_{n-1}}{q_{n-1}}\right) = \tilde{a}_{n-1}.$$

Since $\det(\tilde{M}_n) = -\det M_n = (-1)^{n+1}$, we have $\Delta(f_{\tilde{M}_n}) = \Delta(f)$, i.e.

$$\tilde{b}_n^2 - 4\tilde{a}_n\tilde{c}_n = b^2 - 4ac.$$

Recall the basic inequality

$$\left|\frac{p_n}{q_n} - \alpha\right| < \frac{1}{q_n q_{n+1}} \implies |p_n - q_n\alpha| < \frac{1}{q_{n+1}} < \frac{1}{q_n}.$$

Therefore we can write $p_n = q_n\alpha + \frac{\delta_n}{q_n}$ for some $|\delta_n| < 1$. The coefficient

$$\begin{aligned} \tilde{a}_n &= q_n^2 f\left(\frac{p_n}{q_n}\right) = q_n^2 f\left(\alpha + \frac{\delta_n}{q_n^2}\right) \\ &= q_n^2\left(f'(\alpha)\frac{\delta_n}{q_n^2} + f''(\alpha)\frac{\delta_n^2}{2q_n^4}\right) \text{ (Taylor expansion)} \\ &= f'(\alpha)\delta_n + f''(\alpha)\frac{\delta_n^2}{2q_n^2}. \end{aligned}$$

It follows that $|\tilde{a}_n| < |f'(\alpha)| + |f''(\alpha)|$ and therefore there are finitely many possible values available for $\tilde{a}_n$. Since $\tilde{c}_n = \tilde{a}_{n-1}$, the same holds for $\tilde{c}_n$. On the other hand, we know that $\tilde{b}_n^2 - 4\tilde{a}_n\tilde{c}_n = \Delta(f)$, so $\tilde{b}_n$ can also take only finitely many values. Thus there are only finitely many polynomials $f_{\tilde{M}_n}$ and therefore the set of their roots is finite, which is what we wanted to prove. □

9.3.4 Reduced quadratic numbers and purely periodic continued fractions

Going back to our initial goal, the study of Pell's equations, we can now formulate the following results.

Theorem 9.21. *Let $d > 0$ be a positive integer that is not a square.*

(i) Then the periodic fraction of $\sqrt{d}$ is of the form

$$\sqrt{d} = [a, \overline{b_1, \ldots, b_{m-1}, 2a}]$$

with $b_i = b_{m-i}$ for $1 \leq i \leq m-1$.

(ii) Let

$$\frac{p}{q} = [a, b_1, \ldots, b_{m-1}]$$

written in lowest terms. Then (p, q) is the smallest positive integer solution to the equation

$$x^2 - dy^2 = (-1)^m.$$

(iii) The smallest positive integer solution to Pell's equation

$$x^2 - dy^2 = 1 \tag{9.1}$$

is given by

$$\begin{cases} (p, q) & \text{if } m \text{ is even;} \\ (p^2 + dq^2, 2pq) & \text{if } m \text{ is odd.} \end{cases}$$

(iv) Pell's equation

$$x^2 - dy^2 = -1 \tag{9.2}$$

has positive integer solution if and only if the continued fraction of $\sqrt{d}$ has odd period.

Before we can start proving the theorem, we need some preparation. Consider a number $\alpha = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$.

Definition. *The number $\alpha' = x - y\sqrt{d}$ is called the* conjugate *of α.*

Note that $\alpha = \alpha' \iff \alpha \in \mathbb{Q}$ and $N(\alpha) = \alpha \cdot \alpha'$. Moreover, $(\alpha + \beta)' = \alpha' + \beta'$ and $(\alpha\beta)' = \alpha'\beta'$ for any $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$.

Also note that if $\alpha \notin \mathbb{Q}$ satisfies the quadratic equation

$$a\alpha^2 + b\alpha + c = 0,$$

then the two solutions

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

must be exactly α and α'.

Definition. *A quadratic irrational α is* reduced *if $\alpha > 1$ and $-1 < \alpha' < 0$.*

Example 9.22. Let $r = a/b > 1$ be a rational number that is not a square and consider $\alpha = \sqrt{r} = \sqrt{a/b}$. Then $\alpha > 1$ is a quadratic irrational, but it is not reduced as $\alpha' = -\sqrt{r} = -\alpha < -1$. However, let $a_0 = \lfloor \alpha \rfloor$. Then $\beta = a_0 + \alpha$ is also a quadratic irrational, but $\beta' = a_0 - \alpha \in (-1, 0)$. Hence β is reduced.

Lemma 9.23. *If $\alpha > 1$ and $\alpha' < 0$, then α_n is reduced for every $n \geq 1$.*

Proof. It is enough to prove that α_1 is reduced as the rest follows by induction. Recall that

$$\alpha = a_0 + \frac{1}{\alpha_1}$$

and $a_0 \leq \alpha < a_0 + 1$. Therefore

$$\alpha_1 = \frac{1}{\alpha - a_0} > 1.$$

We also have $\alpha' < 0$ and $a_0 \geq$, so $a_0 - \alpha' > 1$. Hence

$$\alpha_1 = \frac{1}{\alpha' - a_0} \in (-1, 0).$$

□

Theorem 9.24 (Purely periodic continued fraction theorem)**.** *A quadratic irrational α is reduced if and only if α has a purely periodic continued fraction*

$$\alpha = [\overline{a_0, a_1, \ldots, a_n}].$$

In this case, the conjugate α' of α is given by

$$-\frac{1}{\alpha'} = [\overline{a_n, \ldots, a_1, a_0}].$$

Proof. Suppose $\alpha = [\overline{a_0, a_1, \dots, a_n}]$ has a purely periodic continued fraction. Then

$$\begin{aligned}
[a_n, \dots, a_1, a_0] &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & a_n \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & a_1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & a_0 \end{bmatrix} (0) \\
&= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \left(\begin{bmatrix} 0 & 1 \\ 1 & a_0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & a_1 \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & a_n \end{bmatrix} \right)^t (0) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} M_n^t \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} (0) \\
&= \begin{bmatrix} q_n & p_n \\ q_{n-1} & p_{n-1} \end{bmatrix} (0) = \frac{p_n}{p_{n-1}}.
\end{aligned}$$

Thus $\frac{p_n}{p_{n-1}} = [a_n, \dots, a_1, a_0]$ are the convergents of the number $\beta = [\overline{a_n, \dots, a_1, a_0}]$ and β is fixed by the $\tilde{A}_n$ where $A_n = \begin{bmatrix} q_n & p_n \\ q_{n-1} & p_{n-1} \end{bmatrix}$. Thus

$$\beta = \begin{bmatrix} q_n & p_n \\ q_{n-1} & p_n \end{bmatrix} (\beta).$$

Then $\beta > 1$, hence $-\frac{1}{\beta} \in (-1, 0)$. Moreover, β is a root of the polynomial $p_{n-1}X^2 - (q_{n-1} - p_n)X - q_n$. Replacing $X \to -1/X$ we see that $-1/\beta$ is a root of the polynomial

$$f(X) = q_n X^2 - (p_n - q_{n-1})X - p_{n-1}.$$

But

$$\alpha = \tilde{M}_n(\alpha) = \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} (\alpha)$$

is also a root of $f(X)$. Since $\alpha > 1$ and $-1/\beta < 0$ they cannot be equal, so they have to be the two roots of $f(X)$. It follows that $\alpha' = -1/\beta \in (-1, 0)$ and α is reduced. We have also obtained that

$$-\frac{1}{\alpha'} = \beta = [\overline{a_n, \dots, a_1, a_0}].$$

Conversely, assume that α is reduced. Assume that α is not purely periodic. But since it is still a quadratic irrational, Theorem 9.20 tells us that the continued fraction of α is of the form

$$\alpha = [a_0, \dots, a_n, \overline{a_{n+1}, \dots, a_m}]$$

with $m > n$ and $a_m \neq a_n$. By Lemma 9.23, we know that for each $k \geq 1$ the quadratic irrational $\alpha_k = [a_k, a_{k+1}, \dots]$ is reduced. In particular, α_n is reduced. But

$$\alpha_n = [a_n, \overline{a_{n+1}, \dots, a_m}] = a_n + \frac{1}{\alpha_{n+1}}.$$

Therefore

$$\alpha_n' = a_n + \frac{1}{\alpha_{n+1}'} \in (-1, 0) \implies a_n < -\frac{1}{\alpha_{n+1}'} < a_n + 1. \tag{9.11}$$

On the other hand,

$$\alpha_{n+1} = [\overline{a_{n+1}, \dots, a_m}] = \alpha_{m+1}.$$

We also know that

$$\alpha_m = a_m + \frac{1}{\alpha_{m+1}}$$

is reduced, so

$$\alpha'_m = a_m + \frac{1}{\alpha'_{m+1}} = a_m + \frac{1}{\alpha'_{n+1}} \in (-1, 0) \implies a_m < -\frac{1}{\alpha'_{n+1}} < a_m + 1. \tag{9.12}$$

Comparing inequalities (9.11) and (9.12) we see that $a_n = a_m$, a contradiction.

□

Proof of Theorem 9.21 (i). In fact we will prove that the continued fraction of $\alpha = \sqrt{r}$ for $r \in \mathbb{Q}_{>0}$ not a square is of this form. Since r is not a square, α is irrational, so it has an infinite continued fraction

$$\alpha = [a_0, a_1, \dots].$$

Then

$$\alpha = a_0 + \frac{1}{\alpha_1}, \quad \text{where} \quad \alpha_1 = \frac{1}{\alpha - a_0} = [a_1, a_2, \dots].$$

By Example 9.22, we know that $\alpha + a_0$ is reduced, and by Theorem 9.24, it has a purely periodic continued fraction

$$\alpha + a_0 = [\overline{2a_0, b_1, \dots, b_m}]. \tag{9.13}$$

Since $\alpha' = -\alpha$, we also have

$$\alpha_1 = \frac{1}{\alpha - a_0} = -\frac{1}{a_0 - \alpha} = -\frac{1}{a_0 + \alpha'} = [\overline{b_m, \dots, b_1, 2a_0}]. \tag{9.14}$$

Comparing (9.13) and (9.14), we see that $b_i = b_{m-i}$ for $1 \le i \le m-1$ and $b_m = 2a_0$. □

Remark 9.25. The converse is also true: if $\alpha = [a, \overline{b_1, \dots, b_{m-1}, 2a}]$ with $b_i = b_{m-i}$ for $1 \le i \le m-1$, then $\alpha = \sqrt{r}$ for some $r \in \mathbb{Q}_{>0}$ not a square.

Proof. If (9.13) and (9.14) both hold, then

$$\frac{1}{\alpha - a_0} = -\frac{1}{a_0 + \alpha'} \implies \alpha' = -\alpha.$$

□

Proof of Theorem 9.21 (ii). Consider the continued fraction expansion of $\alpha = \sqrt{d}$

$$\alpha = \sqrt{d} = [a, \overline{b_1, \dots, b_{m-1}, 2a}].$$

Then

$$\alpha + a = [\overline{2a, b_1, \dots, b_{m-1}}]$$

is purely periodic. Let $n = km$ for $k \geq 1$. Then

$$\alpha + a = [2a, b_1, \ldots, b_{m-1}, \ldots, 2a, b_1, \ldots, b_{m-1}, \alpha + a].$$

In the matrix version, the first $2a$ plays a different role than the others. To understand this, let us fix some notation. We will denote M_n the matrices corresponding to the continued fraction of α and by A_n the ones corresponding to $\beta = \alpha + a$. Then

$$A_m = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 2a \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & b_1 \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & b_{m-1} \end{bmatrix} = \begin{bmatrix} 1 & 2a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & b_1 \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & b_{m-1} \end{bmatrix}$$

can be rewritten as

$$A_{m-1} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & b_1 \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & b_{m-1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} M_{m-1}.$$

Thus

$$\tilde{A}_{m-1} = A_{m-1} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \tilde{M}_{m-1}$$

fixes $\alpha + a$, i.e.

$$\tilde{A}_{m-1}(\alpha + a) = \alpha + a.$$

It follows that α is fixed by the matrix

$$M = \begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} \tilde{A}_{m-1} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \tilde{M}_{m-1} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} p_{m-1} & p_{m-2} \\ q_{m-1} & q_{m-2} \end{bmatrix} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} p_{m-1} & p_{m-2} + ap_{m-1} \\ q_{m-1} & q_{m-2} + aq_{m-1} \end{bmatrix}.$$

Recall that if α is fixed by the integer matrix

$$M' = \begin{bmatrix} A & B \\ C & D \end{bmatrix},$$

then

$$C\alpha^2 - (A - D)\alpha - B = 0.$$

On the other hand, our particular $\alpha = \sqrt{d}$ is a root of the quadratic equation

$$x^2 - d = 0.$$

Hence we must have $A = D$ and $B = \alpha^2 C$ for any matrix $M' = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ that fixes α. Thus our matrix

$$M = \begin{bmatrix} p_{m-1} & p_{m-2} + ap_{m-1} \\ q_{m-1} & q_{m-2} + aq_{m-1} \end{bmatrix} = \begin{bmatrix} p_{m-1} & dq_{m-1} \\ q_{m-1} & p_{m-1} \end{bmatrix}.$$

Looking at its determinant we see that

$$\det M = p_{m-1}^2 - dq_{m-1}^2 = \det \tilde{M}_{m-1} = (-1)^m$$

and (ii) is proved. □

Proposition 9.26. *Let α be an positive irrational number and a, b be coprime positive integers.*

(*i*) *Suppose $|a - b\alpha| \leq |p_n - q_n\alpha|$ and $0 < b < q_{n+1}$. Then $b = q_n$ and $a = p_n$. Assume a, b are coprime positive integers such that*

$$\left|\frac{a}{b} - \alpha\right| < \frac{1}{2b^2}.$$

Then $\frac{a}{b}$ is one of the convergents s_n of the continued fraction of α.

(*ii*) *Assume*

$$\left|\frac{a}{b} - \alpha\right| < \frac{1}{2b^2}.$$

Then $\frac{a}{b}$ is one of the convergents s_n of the continued fraction of α.

Proof. (*i*) The matrix

$$M_{n+1} = \begin{bmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{bmatrix}$$

had determinant ± 1, so the 2×2 linear system

$$\begin{cases} up_n + vp_{n+1} & = a \\ uq_n + vq_{n+1} & = b \end{cases}$$

has integer solution (u, v). Note that u, v cannot both be positive as that would make $b \geq q_{n+1}$. As a, b are positive, and so are $p_n, p_{n+1}mq_n, q_{n+1}$, we cannot have both u and v negative. Thus $uv \leq 0$.

We have

$$|a - b\alpha| = |up_n + vp_{n+1} - (uq_n + vq_{n+1})\alpha| = |u(p_n - q_n\alpha) + v(p_{n+1} - q_{n+1}\alpha)|.$$

Since consecutive convergence lie on opposite sides of α and $uv \leq 0$, we must have $u(p_n - q_n\alpha)$ and $v(p_{n+1} - q_{n+1}\alpha)$ of the same sign or one of them equal to zero. Therefore the absolute value of their sum is actually equal to the sum of the absolute values and

$$|p_n - q_n\alpha| \geq |a - b\alpha| = |u(p_n - q_n\alpha)| + |v(p_{n+1} - q_{n+1}\alpha)| \implies \begin{cases} \text{either} & |u| = 1 \text{ and } v = 0 \\ \text{or} & u = 0 \end{cases}$$

If $u = 0$, then we must have $b = vq_{n+1} \in (0, q_{n+1})$ which is a contradiction. Hence $v = 0$ and $u = \pm 1$. But $b = qq_n$ and $b, q_n > 0$, so $u = 1$. Thus $b = q_n$ and $a = p_n$.

(*ii*) As the denominators q_n form an increasing unbounded sequence, there exists $n \geq 0$ such that $q_n \leq b < q_{n+1}$. Part (*i*) tells us that the best rational approximation of α with denominator $< q_{n+1}$ is $s_n = \frac{p_n}{q_n}$. Thus we have

$$\frac{1}{2b} > |b\alpha - a| \geq q_n \left|\alpha - \frac{a}{b}\right| \geq q_n|\alpha - s_n| = |q_n\alpha - p_n|.$$

Hence $|x - s_n| < \frac{1}{2bq_n}$. Now suppose that a/b is not a convergent of α, so $\frac{a}{b} \neq s_n$. Thus

$$\frac{1}{bq_n} \geq \frac{|bp_n - aq_n|}{bq_n} = \left|s_n - \frac{a}{b}\right| \leq |s_n - \alpha| + \left|\alpha - \frac{a}{b}\right| < \frac{1}{2bq_n} + \frac{1}{2b^2}.$$

This implies $b < q_n$, which is a contradiction. □

Proposition 9.27. *Let $\alpha = \sqrt{d} \notin \mathbb{Q}$ for a positive integer d. Then for all $n \geq 0$,*

$$\alpha_n = \frac{A_n + \sqrt{d}}{C_n}$$

for some integers A_n, C_n with $B_n > 0$. Moreover

$$p_{n-1}^2 - dq_{n-1}^2 = (-1)^n C_n \quad \text{and} \quad p_n p_{n-1} - q_n q_{n-1} = (-1)^n A_{n+1}. \tag{9.15}$$

Proof. $\alpha_0 = \sqrt{d}$. Then

$$\alpha_1 = \frac{1}{\sqrt{d} - a_0} = \frac{a_0 + \sqrt{d}}{d - a_0^2}$$

and since $d^2 - a_0 > 0$ we are done. Note that $C_0 = 1$ and $A_0 = 0$ and so $C_0 \mid d - A_0^2$. Also $C_1 = d - a_0^2 = \frac{d - A_0^2}{C_0}$ and $A_1 = a_0 = a_0 C_0 - A_0$. Hence $C_1 \mid d - A_1^2$.

An induction argument shows that, for $i \geq 1$ we have

- $1 < \alpha_i = \dfrac{A_i + \sqrt{d}}{C_i}$
- $C_{i+1} = a_i C_i - A_i \in \mathbb{Z}$
- $C_{i+1} = \dfrac{d - A_{i+1}^2}{C_i} \in \mathbb{Z}$
- $C_i \mid d - A_i^2$
- $C_i \neq 0$ (this comes down to $\sqrt{d} \notin \mathbb{Q}$.)
- $C_i > 0$
- $0 < \sqrt{d} - A_i < C_i < \sqrt{d} + A_i < 2\sqrt{d}$.
- $p_{i-1}^2 - dq_{i-1}^2 = (-1)^i C_i$

- $p_i p_{i-1} - q_i q_{i-1} = (-1)^i A_{i+1}$

□

Proof of Theorem 9.21 (iii) and (iv). From Theorem 9.21, part (*ii*), we know that the given pair

$$\begin{cases} (p,q) & \text{if } m \text{ is even} \\ (p^2+dq^2, 2pq) & \text{if } m \text{ is odd} \end{cases}$$

satisfies Pell's equation $x^2 - dy^2 = 1$ and that if m is odd, then (p,q) is a solution of the second Pell equation $x^2 - dy^2 = -1$.

Let (x,y) be a solution to Pell's equation $x^2 - dy^2 = \pm 1$ with $x > 1, y \geq 0$.

Then

$$\left| \frac{x}{y} - \sqrt{d} \right| = \frac{1}{|y(x + y\sqrt{d})|} = \frac{1}{y^2(\sqrt{d} + \sqrt{1/y^2 + d})}.$$

Note that $\sqrt{d} + \sqrt{1/y^2 + d} > 2\sqrt{d} > 2$ and the above equality implies that

$$\left| \frac{x}{y} - \sqrt{d} \right| < \frac{1}{2y^2}.$$

By Proposition 9.26, this implies that x/y is a convergent for $\sqrt{d}$, i.e. there exists $n \geq 0$ such that $x = p_n$ and $y = q_n$.

Now want to show that $\alpha_n \in \mathbb{Z}[\sqrt{d}]$ only when n is a multiple of m. But $\alpha_n \in \mathbb{Z}[\sqrt{d}] \iff C_n = 1 \implies \lambda_{n+1} = \alpha_n - a_n = \frac{A_n + \sqrt{d}}{C_n} - a_n = (A_n - a_n) + \sqrt{d}$. As $\lambda_{n+1} \in (0,1)$ it follows that $A_n - a_n = -\lfloor \sqrt{d} \rfloor$ and $\lambda_{n+1} = \sqrt{d} - \lfloor \sqrt{d} \rfloor = \lambda_1$. Thus n is multiple of the period m of $\sqrt{d}$.

Thus (9.15) implies that (p_{n-1}, q_{n-1}) is a solution of the Pell's equation

$$x^2 - y^2 d = 1$$

if and only if n is a multiple of m and n is even. As $p_{m-1} = p$ and $q_{m-1} = q$ and $p_{2m-1} + q_{2m-1}\sqrt{d} = (p_{m-1} + q_{m-1}\sqrt{d})^2$ part (*iii*) is proved. The same relation (9.15) also implies that (p_{n-1}, q_{n-1}) is a solution of the other Pell equation

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

if and only if n is a multiple of m and n is odd. Note that m has odd multiples only when it is odd itself, so (*iv*) is proved as well.

□

9.4 Other applications of continued fractions

Continued fractions crop up in many areas of number theory besides the standard application to Pell's equation. They can be used to break RSA encryption if the decryption key is too small, prove sum of two squares theorems, to recognize rational numbers, or to prove transcendence results.

RSA Encryption

Recall that in RSA encryption, Bob picks two large primes p and q that satisfy $p < q < 2p$. Then he computes $N = pq$. (The inequality is necessary when doing cryptography, since there are specialized factoring algorithms that can exploit when N is a product or primes of significantly different magnitude.) Using the factorization of N, Bob picks encryption and decryption keys e and d that satisfy $e \equiv d^{-1} (\text{mod } \phi(N))$. Bob publishes N and e, but keeps d, p and q secret. To encrypt a message m, Alice encodes it as a number modulo N and gives Bob $c \equiv m^e (\text{mod } N)$. Bob calculates $c^d \equiv m (\text{mod } N)$ to decrypt the message. There is no known way to recover the message in general without factoring N and no known way to factor N efficiently.

However, if it so happens that $3d < N^{1/4}$, any adversary can find e using only N and e. Let $kin\mathbb{Z}_{\geq 0}$ such that $ed - 1 = k\phi(N)$. Since $e < \phi(N)$, we have $k < d$. Given that we chose $p < q < 2p$, we have $p < \sqrt{pq} = \sqrt{N}$ and $q < \sqrt{2N}$. Thus $p + q < 3\sqrt{N}$ and

$$\left| \frac{e}{N} - \frac{k}{d} \right| \leq \frac{|k\phi(N) + 1 - Nk|}{Nd} = \frac{|k(N - p - q + 1) + 1 - Nk|}{Nd} = \frac{k(p + q - 1) + 1}{Nd} \leq \frac{3k}{d\sqrt{N}} < \frac{1}{3d^2}.$$

This inequality implies that $\frac{k}{d}$ is a convergent to $\frac{e}{N}$ (by Proposition 9.26). Using the publicly available e and N, an adversary can use the Euclidean algorithm to find all the convergents with denominator less than N in time poly-logarithmic in N. For each convergent, use its numerator and denominator as a guess for k and d, and calculate what $\phi(N)$ should be. Since p and q satisfy the quadratic

$$x^2 - (N - \phi(N) + 1)x + n = 0,$$

the correct guess of $\phi(N)$ will give the factorization of N.

Recognizing Rational Numbers

Continued fractions also give a way to recognize decimal approximations of rational numbers. Since a rational number has a finite continued fraction, to check whether a given decimal approximation probably comes from a rational number, run the continued fraction algorithm on the decimal approximation. If the decimal is approximating a rational, when the continued fraction algorithm should have terminated after the nth step, there will instead be a very tiny error between $[a_0, a_1, \ldots, a_n]$ and the decimal approximation. This will result in a huge value for the a_{n+1}. Looking for huge a_i provides a way to find possible rational numbers that the decimal would be approximating.

For example, a simple calculation shows that

$$\frac{1003}{957} = [1, 20, 1, 4, 9].$$

Approximating the fraction to 100 binary digits gives

$$1.0480668756530825496342737722\,.$$

Changing the last digit to a 3 and running the continued fraction algorithm (with a computer, of course) gives

$$[1, 20, 1, 4, 9, 10789993838034437479169],$$

so we can identify it as the fraction

$$[1, 20, 1, 4, 9] = \frac{1003}{957}.$$

Note that the fraction is identified although the decimal expansion has not started repeating.

10 Primes of the form $p = x^2 + ny^2$

In Section 7.2 we proved that a prime p can be written as the sum of two squares if and only if $p = 2$ or $p \equiv 1 \pmod 4$. One direction was easy, but the other one was completely non-trivial. The proof consisted of two steps.

Reciprocity step: A prime $p \equiv 1 \pmod 4$, then it divides $N = a^2 + b^2$ with a and b relatively prime integers.

The proof was a bit ad-hoc. We used the fact that $4 \mid \phi(p)$ to find an integer a for which $a^2 + 1 \equiv 0 \pmod p$.

Descent step: If a prime p divides a number N of the form $N = a^2 + b^2$, where $(a, b) = 1$, then p itself can be written as $p = x^2 + y^2$ for some $(x, y) = 1$.

This step was based on Lemma 7.6 which said that if a prime $q = x^2+y^2$ divides a sum of squares $a^2 + b^2 = N$ with $(a, b) = 1$, then N/q can be written as a sum of relatively prime squares.

Furthermore, we used in an essential way the fact that if a number N is the sum of two squares, then all its prime divisors can be written as sums of two squares.

One can look at other questions of this type. For instance, Fermat himself stated (and Euler proved) the following two results.

Theorem 10.1. *A prime p is of the form $p = x^2 + 2y^2$ if and only if $p = 2$ or $p \equiv 1$ or $3 \pmod 8$.*

Theorem 10.2. *A prime p is of the form $p = x^2+3y^2$ if and only if $p = 3$ or $p \equiv 1 \pmod 3$.*

Again, it is easy to show that if the prime has the given form in terms of squares, then it lands in the desired congruence class. For the other direction, let us try to imitate the procedure from Section 7.2.

Descent step

We start by considering the generalization of the Lemma 7.6. This is the first component of our descent step.

Lemma 10.3. *Fix $n \in \mathbb{Z}_{>0}$. Suppose M is an integer of the form $M = a^2 + nb^2$ with $(a, b) = 1$ and that $q = x^2 + ny^2$ is a prime divisor of M. Then there exist integers $(c, d) = 1$ such that $M/q = c^2 + nd^2$.*

Proof. The general case is one of the homework problems. Here we discuss only the proof in the case $n = 2$.

We know that $M = a^2 + 2b^2, (a, b) = 1, q = x^2 + 2y^2$ is prime and $q \mid M$. Since q is prime x and y are forced to be relatively prime. Just as in the proof of Lemma 7.6 we look at

$$x^2M - 2b^2q = x^2(a^2 + 2b^2) - 2b^2(x^2 + 2y^2) = (ax - 2by)(ax + 2by).$$

Since $q \mid (x^2M - 2b^2q)$ it follows that $q \mid (ax - 2by)$ or $q \mid (ax + 2by)$. Without loss of generality (we can always change the sign of b), we can assume that

$$q \mid ax - 2by.$$

Thus, there exist an integer d such that $ax - 2by = dq$. We can rewrite this as

$$2by = ax - dq = ax - dx^2 - 2dy^2,$$

which implies that $x \mid 2y(b + dy)$. Not only is x relatively prime to y, but it is also odd (if x is even then q cannot be prime). Therefore $x \mid (b + dy)$, so

$$b + dy = cx$$

for some integer c. On the other hand, $2cxy = 2y(b + dy) = x(a - dx)$, so

$$a - dx = 2cy.$$

But then

$$M = a^2 + 2b^2 = (dx + 2cy)^2 + 2(cx - dy)^2 = (x^2 + 2y^2)(c^2 + 2d^2) = q(c^2 + 2d^2).$$

Note that since $(a, b) = 1$ we must also have $(c, d) = 1$. □

And now we try to reproduce the second component of the descent step. That is we would like to say that

$$p \text{ prime}, p \mid a^2 + nb^2 \text{ with } (a, b) = 1 \implies p = x^2 + ny^2. \tag{10.1}$$

As in the Section 7.2 we can assume that

$$|a|, |b| \leq \frac{p}{2}.$$

Then, if p is odd

$$a^2 + nb^2 < \frac{n+1}{4}p^2.$$

If $n \leq 3$, this implies that $a^2 + nb^2 < p^2$ and therefore any prime divisor $q \neq p$ of $a^2 + nb^2$ has to be $q < p$. Now we can complete the descent step using the same argument as in Section 7.3.2.

For $n = 1$: done in Section 7.3.2.

For $n = 2$: assume that p cannot be written as

$$x^2 + 2y^2. \tag{10.2}$$

If all the other prime divisors of $a^2 + 2b^2$ could be written in the form (10.2), then Lemma 10.3 would imply that p can also be written as in (10.2) and we assumed that this is not the case. (Here we used that $p^2 \nmid a^2 + 2b^2$ because $a^2 + 2b^2 < p^2$.) Hence there must exist a prime divisor $p_1 \neq p$ of $a^2 + 2b^2$ that cannot be expressed as (10.2). But we have seen that any other prime divisor p_1 of $a^2 + 2b^2$ has to be $p_1 < p$. By the same argument now there must exist yet another prime $p_2 < p_1 < p$ that cannot be written in the given form (10.2). And then another, and another... There is nothing to prevent us from repeating this process indefinitely (note that 2 is of the desired form) and thus we get an infinite decreasing sequence of positive (and prime) numbers. This contradiction finishes the descent step.

For $n = 3$: see the homework problems.

Note that (10.1) *cannot* hold in general. For instance, in the case $n = 5$ we see that $3 \mid 21 = 1^2 + 5 \cdot 2^2$, but 3 cannot be written as $x^2 + 5y^2$. So we need to figure out how the prime divisors of $a^2 + nb^2$ can be represented. The answer will come from Legendre's theory of reduced quadratic forms.

Reciprocity step

We need to find congruence conditions which will guarantee that $p \mid x^2 + ny^2$ for some $(x, y) = 1$.

The problem is that we cannot adapt directly our proof from the $n = 1$ case (Section 7.2). This is because our proof was done in an ad-hoc manner. Namely, to recap, we said that if $p \equiv 1 \pmod 4$, then $\phi(p) = 4k$ for some integer k. Therefore the polynomial $X^{4k} - 1$ has $4k$ roots $\pmod p$. But

$$X^{4k} - 1 = (X^{2k} - 1)(X^{2k} + 1).$$

Since $X^{2k} - 1$ can have at most $2k$ roots $\pmod p$, it follows that there must exist an integer $(a, p) = 1$ such that $a^{2k} + 1 \equiv 0 \pmod p$. Thus $p \mid (a^k)^2 + 1^2$ and since a^k and 1 are relatively prime, we are done.

But this cannot be replicated directly for $n = 2$ for instance.

One more thing that is worth noticing. We have the following conjectures (due to Fermat).

- $n = 1 : p \equiv 1 \pmod 4 \implies p \mid a^2 + b^2$ for some $(a, b) = 1$.

- $n = 2 : p \equiv 1, 3 \pmod 8 \implies p \mid a^2 + 2b^2$ for some $(a, b) = 1$.

- $n = 3 : p \equiv 1 \pmod 3 \implies p \mid a^2 + 3b^2$ for some $(a, b) = 1$.

The key observation is that these are all congruences modulo $4n$. (The last one can be restated as $p \equiv 1, 7 \pmod{12}$.) And indeed, we are going to find conditions $\pmod{4n}$ that would ensure that a prime p is of the form x^2+ny^2. A systematic approach will be formulated in terms of the Legendre symbol (see Section 11).

11 Quadratic reciprocity

11.1 Legendre symbol

In this section p will be an *odd* prime.

Definition. *An integer $a \not\equiv 0 \pmod p$ is called a* quadratic residue *modulo p if there exist $x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod p$; otherwise the integer $a \not\equiv 0 \pmod p$ is called a* quadratic nonresidue *modulo p.*

Note that the definition depends only on the residue class of $a \pmod p$.

Example

	$p = 3$	$p = 5$	$p = 7$
quadratic residues	1	$1, 4$	$1, 2, 4$
quadratic nonresidues	2	$2, 3$	$3, 5, 6$

Lemma 11.1. *In any reduced residue system modulo p, there are exactly $\frac{p-1}{2}$ quadratic residue and $\frac{p-1}{2}$ quadratic nonresidues.*

Proof. Exercise. □

Note: We could try to make a similar definition modulo an odd positive integer n. But Lemma 11.1 would not hold. For instance, if we take $n = 15$ we have 8 modulo classes relatively prime to $15 : 1, 2, 4, 7, 8, 11, 13, 14$. But only 1 and 4 are quadratic residues.

Definition. *The Legendre symbol modulo p is the function $\mathbb{Z} \to \mathbb{C}$ given by*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue} \pmod p \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic nonresidue} \pmod p. \end{cases}$$

Example

$$\left(\frac{1}{3}\right) = 1 \quad \left(\frac{2}{3}\right) = -1 \quad \left(\frac{-43}{3}\right) = \left(\frac{2}{3}\right) = 1 \quad \left(\frac{2}{7}\right) = 1 \quad \left(\frac{14}{7}\right) = 0$$

In general $\left(\frac{1}{p}\right) = 1$ for any odd prime p.

The connection to the reciprocity step in Section 10 is provided by the following fact.

Proposition 11.2. *Let n be an integer relatively prime to p. Then*

$$p \mid a^2 + nb^2 \text{ for some integers } (a,b) = 1 \iff \left(\frac{-n}{p}\right) = 1.$$

Proof. First assume that there exist integers $(a,b) = 1$ such that $a^2 + nb^2 \equiv 0 \pmod{p}$. Since a and b are relatively prime, it follows that $b \not\equiv 0 \pmod{p}$. Therefore there exist $c \in \mathbb{Z}$ such that $bc \equiv 1 \pmod{p}$. But then

$$a^2c^2 + n \equiv 0 \pmod{p} \implies \left(\frac{-n}{p}\right) = 1.$$

The other direction is even simpler. Since $-n$ is a quadratic residue $\pmod{p}$, there exists an integer a such that $a^2 \equiv -n \pmod{p}$. Hence $p \mid a^2 + n \cdot 1^2$ and $(a,1) = 1$. □

Corollary 11.3.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4}. \end{cases}$$

Proof. Follows immediately from Proposition 11.2 and Theorem 7.4. □

Lemma 11.4 (Euler's criterion)**.**

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

Proof. If $p \mid a$ we get 0 on both sides and the equality holds.
If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$, so $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. We have two cases.

- If $\left(\frac{a}{p}\right) = 1$, there exists $x \not\equiv 0 \pmod{p}$ such that $a \equiv x^2 \pmod{p}$, so

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

- If $\left(\frac{a}{p}\right) = -1$, it is enough to show that $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. Consider the polynomial

$$f(X) = X^{\frac{p-1}{2}} - 1.$$

It has at most $\frac{p-1}{2}$ roots modulo p. On the other hand, we have seen from the previous case that all the quadratic residues are roots of $f(X)$. By Lemma 11.1, there are exactly $\frac{p-1}{2}$ quadratic residues $\pmod{p}$. Hence no quadratic nonresidue can be a root of $f(X)$, and we are done.

□

Proposition 11.5. *The Legendre symbol modulo p is a completely multiplicative function.*

Proof. We apply Euler's criterion twice.

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

The result follows since $1 \not\equiv -1 \pmod{p}$ and $0 \not\equiv \pm 1 \pmod{p}$. □

Proposition 11.6.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8}. \end{cases}$$

Proof. By Euler's criterion we know that

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

There are exactly $\frac{p-1}{2}$ *even* integers between 1 and p. We have the following congruences for them.

$$\begin{array}{ll} p-1 \equiv 1(-1)^1 \pmod{p} & 2 \equiv 2(-1)^2 \pmod{p} \\ p-3 \equiv 3(-1)^3 \pmod{p} & 4 \equiv 4(-1)^4 \pmod{p} \\ \vdots & \vdots \end{array}$$

One of the columns will end with either $p - \frac{p-1}{2}$ or $\frac{p-1}{2}$ (whichever one is even). Taking the product of all these relations we obtain

$$2 \cdot 4 \cdots (p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+\ldots+\frac{p-1}{2}} \pmod{p},$$

which can be rewritten as

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

Since $p \nmid \left(\frac{p-1}{2}\right)!$ this simplifies to

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$$

and the desired result follows. □

Corollary 11.7.

$$p \mid a^2 + 2b^2 \text{ for some integers } (a,b) = 1 \iff p \equiv 1, 3 \pmod{8}.$$

Proof. By Proposition 11.2 we know that

$$p \mid a^2 + 2b^2 \text{ for some integers } (a,b) = 1 \iff \left(\frac{-2}{p}\right) = 1,$$

so all we need to do is figure out for which residue classes (mod 8) the Legendre symbol $\left(\frac{-2}{p}\right)$ is equal to 1. Since the Legendre symbol is completely multiplicative we have

$$\left(\frac{-2}{p}\right) = 1 \iff \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1 \iff \left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) \iff (-1)^{\frac{p-1}{2}} = (-1)^{\frac{p^2-1}{8}}.$$

In other words, we need to see when

$$\frac{p-1}{2} \equiv \frac{p^2-1}{8} \pmod{2}.$$

If $p = 8k+1$,	then	$\frac{p-1}{2} = 4k$,	$\frac{p^2-1}{8} = 8k^2 + 2k$	both even
If $p = 8k+3$,	then	$\frac{p-1}{2} = 4k+1$,	$\frac{p^2-1}{8} = 8k^2 + 6k + 1$	both odd
If $p = 8k+5$,	then	$\frac{p-1}{2} = 4k+2$,	$\frac{p^2-1}{8} = 8k^2 + 10k + 3$	one even, one odd
If $p = 8k+7$,	then	$\frac{p-1}{2} = 4k+3$,	$\frac{p^2-1}{8} = 8k^2 + 14k + 6$	one odd, one even

□

The above Corollary, together with the descent step for $n = 2$ that we proved in Section 10, proves Theorem 10.1.

Lemma 11.8 (Gauss's Lemma)**.** *Assume $n \not\equiv 0 \pmod{p}$. For $1 \le t \le \frac{p-1}{2}$ denote by x_t the remainder of the division of tn by p. Let*

$$m = \#\left\{x_t; x_t > \frac{p}{2}, 1 \le t \le \frac{p-1}{2}\right\}.$$

Then

$$\left(\frac{n}{p}\right) = (-1)^m.$$

Proof. Denote $r = \dfrac{p-1}{2}$.

First note that $x_1, \ldots, x_r$ are distinct integers between 1 and $p-1$. Indeed, since they are remainders to divisions by p, then have to be $0 \leq x_t \leq p-1$.

On the other hand, since $p \nmid n$, p cannot divide any of the integers

$$n, 2n, 3n, \ldots, \frac{p-1}{2}n.$$

So $x_t \geq 1$ for all $1 \leq t \leq \dfrac{p-1}{2}$. On the other hand, if $x_t = x_s$ for some $1 \leq s, t \leq \frac{p-1}{2}$, we must have $tn \equiv sn \pmod{p}$. This means $p \mid t-s$ and given the range of possible values for s and t, the only way this could happen is for $s = t$.

Denote by A the set of x_t's that are $< p/2$ and by B the set of x_t's that are $> p/2$.

Note that by definition $m = \#B$. Denote $k = \#A$. Since $A \cup B = \{x_1, \ldots, x_r\}$ and $A \cap B = \emptyset$ and not two x_t's are the same, it follows that

$$k + m = r = \frac{p-1}{2}.$$

Denote by $a_1, \ldots, a_k$ the elements of A and by $b_1, \ldots, b_m$ the elements of B. Let

$$C = \{c_1, \ldots, c_m\} \text{ where } c_j = p - b_j,\ 1 \leq j \leq m.$$

Then $\#C = m$ and both

$$A, C \subset \left\{1, 2, \ldots, \frac{p-1}{2}\right\}. \tag{11.1}$$

Claim $A \cap C = \emptyset$.

If we had $a_i = c_j$ for some $1 \leq i \leq k$ and some $1 \leq j \leq m$, then $a_i + b_j = p$. By the very definition of the sets A and B, there exist integers $1 \leq s, t \leq \dfrac{p-1}{2}$ such that $a_i = x_s \equiv sn \pmod{p}$ and $b_j = x_t \equiv tn \pmod{p}$. Therefore

$$sn + tn \equiv 0 \pmod{p}.$$

Since $(n, p) = 1$, this means that $p \mid s+t$. But this is impossible given that $0 < s+t \leq p-1$.

The claim implies that

$$\#A \cup C = m + k = \frac{p-1}{2}. \tag{11.2}$$

Taken together, (11.1) and (11.2) imply that

$$A \cup C = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}.$$

Therefore the product of all elements of $A \cup C$ is

$$a_1 \cdots a_k c_1 \cdots c_m = \left(\frac{p-1}{2}\right)!$$

Therefore

$$\left(\frac{p-1}{2}\right)! \equiv a_1 \cdots a_k (-b_1) \cdots (-b_m) \pmod{p} \equiv (-1)^m a_1 \cdots a_k b_1 \cdots b_m \pmod{p}$$

Going back to the definition of the sets A and B, this can be rewritten as

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^m \prod_{1 \le t \le r} x_t \pmod{p} \equiv (-1)^m \prod_{1 \le t \le r} tn \pmod{p}.$$

Hence

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

Since $\left(\frac{p-1}{2}\right)! \not\equiv 0 \pmod{p}$, multiplying both sides by $(-1)^m$ gives us

$$(-1)^m \equiv n^{\frac{p-1}{2}} \pmod{p},$$

and the result follows from Euler's criterion (Lemma 11.4).

□

Note that we are interested only in the parity of m. The following result deals with said parity.

Proposition 11.9. *Let n be an integer not divisible by p. With the same notation as in Gauss's Lemma 11.8, we have*

$$m \equiv \left((n-1)\frac{p^2-1}{8} + \sum_{1 \le t \le \frac{p-1}{2}} \left\lfloor \frac{tn}{p} \right\rfloor \right) \pmod{2}.$$

In particular, if n is odd, then

$$m \equiv \left(\sum_{1 \le t \le \frac{p-1}{2}} \left\lfloor \frac{tn}{p} \right\rfloor \right) \pmod{2}.$$

Proof. Denote

$$\gamma = \sum_{1 \le t \le \frac{p-1}{2}} \left\lfloor \frac{tn}{p} \right\rfloor.$$

We will use the same notation from the proof of Gauss's Lemma 11.8. For each $1 \leq t \leq \frac{p-1}{2}$, we have

$$\frac{tn}{p} = \left\lfloor \frac{tn}{p} \right\rfloor + \left\{ \frac{tn}{p} \right\}$$

and the fractional part is strictly between 0 and 1. It follows that

$$x_t = p\left\{ \frac{tn}{p} \right\} = \frac{tn}{p} - \left\lfloor \frac{tn}{p} \right\rfloor. \tag{11.3}$$

Recall that we defined sets $A = \{a_1, \ldots, a_k\}, B = \{b_1, \ldots, b_m\}$ and $C = \{c_1, \ldots, c_m\}$ with $c_j = p - b_j, 1 \leq j \leq m$. By definition, A and B are disjoint and their union is $\left\{x_t; 1 \leq t \leq \frac{p-1}{2}\right\}$, so

$$\sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j = \sum_{1 \leq t \leq \frac{p-1}{2}} x_t.$$

Let $\alpha = \sum_{i=1}^{k} a_i$ and $\beta = \sum_{j=1}^{m} b_j$. Substituting (11.3) above we get that

$$\alpha + \beta = \left(\sum_{1 \leq t \leq \frac{p-1}{2}} tn \right) - p\left(\sum_{1 \leq t \leq \frac{p-1}{2}} \left\lfloor \frac{tn}{p} \right\rfloor \right) = n\frac{p^2-1}{8} - p\gamma. \tag{11.4}$$

We have also seen that the sets A and C are disjoint and their union is $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. Therefore

$$\sum_{i=1}^{k} a_i + \sum_{j=1}^{m} c_j = \sum_{1 \leq t \leq \frac{p-1}{2}} t = \frac{p^2-1}{8}.$$

We can rewrite this as

$$\alpha + \sum_{j=1}^{m} (p - b_j) = \frac{p^2-1}{8},$$

which implies that

$$\alpha - \beta + pm = \frac{p^2-1}{8}. \tag{11.5}$$

Adding up (11.4) and (11.5) yields

$$2\alpha + pm = (n+1)\frac{p^2-1}{8} - p\gamma.$$

When we reduce this $\pmod 2$, taking into account that p is odd, we obtain

$$m \equiv pm \pmod 2 \equiv (n+1)\frac{p^2-1}{8} - p\gamma \pmod 2 \equiv (n-1)\frac{p^2-1}{8} + \gamma \pmod 2.$$

□

Theorem 11.10 (Quadratic reciprocity law)**.** *If p and q are odd primes, then*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

Proof. If the two primes are equal, the relation obviously holds. If they are different, then the Legendre symbols are nonzero, and so the relation is equivalent to

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}. \tag{11.6}$$

By Gauss's Lemma 11.8 and Proposition 11.9, the two Legendre symbols are

$$\left(\frac{q}{p}\right) = (-1)^{m_1} \qquad \text{where} \qquad m_1 \equiv \sum_{1\le t\le \frac{p-1}{2}} \left\lfloor \frac{tq}{p} \right\rfloor \pmod 2;$$

$$\left(\frac{p}{q}\right) = (-1)^{m_2} \qquad \text{where} \qquad m_2 \equiv \sum_{1\le s\le \frac{q-1}{2}} \left\lfloor \frac{sp}{q} \right\rfloor \pmod 2.$$

Hence (11.6) would follow if we proved that

$$\sum_{1\le t\le \frac{p-1}{2}} \left\lfloor \frac{tq}{p} \right\rfloor + \sum_{1\le s\le \frac{q-1}{2}} \left\lfloor \frac{sp}{q} \right\rfloor = \frac{p-1}{2}\,\frac{q-1}{2}. \tag{11.7}$$

To this end, consider the function $f(x,y) = qx - py$ on the domain $|x| < \frac{p}{2}, |y| < \frac{q}{2}$. A couple of observations about $f(x,y)$ are in order.

- $x, y \in \mathbb{Z} \implies f(x,y) \in \mathbb{Z}$.
- $(x_1, y_1) \neq (x_2, y_2)$ pairs of integers in our domain $\implies f(x_1, y_1) \neq f(x_2, y_2)$.

The first observation is immediate. For the second, note that, if $f(x_1, y_1) = f(x_2, y_2)$ then $q(x_1 - x_2) = p(y_1 - y_2)$. Thus $p \mid x_1 - x_2$ and $q \mid y_1 - y_2$. Given the range in which these integers live, this is possible only if $x_1 - x_2 = 0$ and $y_1 - y_2 = 0$.

Therefore $f(x,y)$ takes $\frac{p-1}{2} \cdot \frac{q-1}{2}$ nonzero values as the integer x ranges from 1 to $\frac{p-1}{2}$ and the integer y ranges from 1 to $\frac{q-1}{2}$. Now we count the number of positive and negative values of $f(x,y)$ in this range. Fix the integer $1 \le x \le \frac{p-1}{2}$. Then

$$f(x,y) > 0 \iff qx > py \iff y < \frac{qx}{p} \iff 1 \le y \le \left\lfloor \frac{tx}{p} \right\rfloor$$

and so, the number of positive values that $f(x,y)$ takes is precisely

$$\sum_{1\le x\le \frac{p-1}{2}} \left\lfloor \frac{tx}{p} \right\rfloor.$$

Similarly, fix an integer $1 \le y \le \frac{q-1}{2}$. Then

$$f(x,y) < 0 \iff qx < py \iff x < \frac{py}{q} \iff 1 \le x \le \left\lfloor \frac{py}{q} \right\rfloor,$$

and the number of negative values that $f(x,y)$ takes is

$$\sum_{1 \le y \le \frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor.$$

Therefore (11.7) holds and the theorem is proved. □

Note: This proof has a nice interpretation in terms of lattice points in the plane. Find it!

Example: Determine whether 583 is a quadratic residue or nonresidue (mod 907).

$$\left(\frac{583}{907}\right) = \left(\frac{11}{907}\right)\left(\frac{53}{907}\right) = (-1)^{\frac{11-1}{2}\frac{907-1}{2}}\left(\frac{907}{11}\right)(-1)^{\frac{53-1}{2}\frac{907-1}{2}}\left(\frac{907}{53}\right) = -\left(\frac{5}{11}\right)\left(\frac{6}{53}\right)$$
$$= -(-1)^{\frac{5-1}{2}\frac{11-1}{2}}\left(\frac{11}{5}\right)\left(\frac{2}{53}\right)\left(\frac{3}{53}\right) = -\left(\frac{1}{5}\right)(-1)^{\frac{(53-1)(53+1)}{8}}(-1)^{\frac{53-1}{2}\frac{3-1}{2}}\left(\frac{53}{3}\right) = \left(\frac{2}{3}\right) = -1$$

Therefore 583 is a quadratic **non**residue (mod 907).

Now we are ready to prove the reciprocity step for primes of the form $x^2 + 3y^2$. For that, we need to figure out for which primes 3 is a quadratic residue, and for which it is not. For $p > 3$ we have

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

The first factor yields a condition modulo 4, while the second yields a condition modulo 3. Thus we need to look at congruence classes modulo 12. There are four cases.

$p \pmod{12}$	$p \pmod 4$	$p \pmod 3$	$(-1)^{\frac{p-1}{2}}$	$\left(\frac{p}{3}\right)$	$\left(\frac{3}{p}\right)$	$\left(\frac{-3}{p}\right)$
1	1	1	1	1	1	1
5	1	2	1	−1	−1	−1
7	3	1	−1	1	−1	1
11	3	2	−1	−1	1	−1

Here we used the fact that

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

Therefore, Proposition 11.2 implies the reciprocity step for $n = 3$ below.

Proposition 11.11. *Let $p > 3$ be a prime. Then*

$$p \mid a^2 + 3b^2 \text{ for some integers } (a, b) = 1 \iff p \equiv 1, 7 \pmod{12}.$$

The above result, together with the descent step outlined in Problem 4 of Homework 8, prove Theorem 10.2.

The general problem of which primes can be written as $x^2 + ny^2$ with n a fixed positive integer is more complicated though. However, quadratic reciprocity allows us to get closer to our goal of understanding the reciprocity step.

Proposition 11.12. *If p and q are distinct odd primes, then*

$$\left(\frac{q}{p}\right) = 1 \iff p \equiv \pm a^2 \pmod{4q} \text{ for some odd integer } a.$$

Proof. Let $p^* = (-1)^{\frac{p-1}{2}} p$. Then

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

But we know that

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}},$$

and therefore

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

By quadratic reciprocity (Theorem 11.10),

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Therefore it remains to prove that

$$\left(\frac{p^*}{q}\right) = 1 \iff p \equiv \pm a^2 \pmod{4q} \text{ for some odd integer } a.$$

The proof of this last equivalence is left as an exercise. □

11.2 Jacobi symbol

In order to move forward toward our goal of completing the reciprocity step in Euler's strategy we need to extend the Legendre symbol beyond primes. This extension is due to Jacobi.

Definition. *Let m be an odd positive integer.*

- *If $m = 1$, the Jacobi symbol $\left(\frac{\cdot}{1}\right) : \mathbb{Z} \to \mathbb{C}$ is the constant function 1.*
- *If $m > 1$, it has a decomposition as a product of (not necessarily distinct) primes $m = p_1 \cdots p_r$. The Jacobi symbol $\left(\frac{\cdot}{m}\right) : \mathbb{Z} \to \mathbb{C}$ is given by*

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

Note: The Jacobi symbol does not necessarily distinguish between quadratic residues and nonresidues. That is, we could have $\left(\frac{a}{m}\right) = 1$ just because two of the factors happen to be -1. For instance,

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1,$$

but 2 is not a square modulo 15. The following properties of the Jacobi symbol are direct consequences of its definition.

Proposition 11.13. *Let m, n be positive odd integers and $a, b \in \mathbb{Z}$. Then*

(i) $\left(\frac{1}{m}\right) = 1$;

(ii) $\left(\frac{a}{m}\right) = 0 \iff (a, m) > 1$;

(iii) $a \equiv b \pmod{m} \implies \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$;

(iv) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$;

(v) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$;

(vi) $(a, m) = 1 \implies \left(\frac{a^2 b}{m}\right) = \left(\frac{b}{m}\right)$.

Proof. Exercise. □

Theorem 11.14. *Let m, n be positive odd integers. Then*

(i) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$;

(ii) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$;

(iii) $\left(\dfrac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\dfrac{m}{n}\right)$.

Proof. The first two formulas are trivially true when $m = 1$ and so is the third if $m = 1$ or $n = 1$ or if $(m, n) > 1$. We assume that $m, n > 1$ and $(m, n) = 1$.
Thus $m = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$ for some primes p_i and q_j and $p_i \neq q_j$ for all $1 \leq i \leq r, 1 \leq j \leq s$. Then

$$m = \prod_{i=1}^{r} p_i = \prod_{i=1}^{r} (1 + (p_i - 1)) = 1 + \sum_{i=1}^{r} (p_i - 1) + \sum_{1 \leq i_1 < i_2 \leq r} (p_{i_1} - 1)(p_{i_2} - 1) +$$
$$\ldots \text{ products of } 3, 4 \text{ and so on factors } \ldots$$

Since m is odd, so are the primes p_i. Therefore $p_i - 1 \equiv 0 \pmod 2$ and $(p_{i_1} - 1)(p_{i_2} - 1) \equiv 0 \pmod 4$. Therefore all the terms in the above sum that are implicit are also divisible by 4. Hence

$$m \equiv 1 + \sum_{i=1}^{r} (p_i - 1) \pmod 4,$$

which is to say

$$m - 1 \equiv \sum_{i=1}^{r} (p_i - 1) \pmod 4.$$

Since m and the p_i's are odd, it follows that $m - 1 \equiv 0 \pmod 2$ and $p_1 - 1 \equiv 0 \pmod 2, 1 \leq i \leq r$. Thus we can divide each term above by 2 and still get integers. It follows that

$$\frac{m-1}{2} \equiv \sum_{i=1}^{r} \frac{p_i - 1}{2} \pmod 2, \tag{11.8}$$

so

$$(-1)^{\frac{m-1}{2}} = (-1)^{\sum_{i=1}^{r} \frac{p_i - 1}{2}} = \prod_{i=1}^{r} (-1)^{\frac{p_i - 1}{2}} = \prod_{i=1}^{r} \left(\frac{-1}{p_i}\right) = \left(\frac{-1}{m}\right).$$

Similarly,

$$m^2 = \prod_{i=1}^{r} p_i^2 = \prod_{i=1}^{r} \left(1 + (p_i^2 - 1)\right) = 1 + \sum_{i=1}^{r} (p_i^2 - 1) + \sum_{1 \leq i_1 < i_2 \leq r} (p_{i_1}^2 - 1)(p_{i_2}^2 - 1) +$$
$$\ldots \text{ products of } 3, 4 \text{ and so on factors } \ldots$$

We use again the fact that both m and the p_i are odd. That means that $m^2 - 1 = (m - 1)(m + 1)$ is the product of two consecutive even integers, so one of them is divisible by 4. Thus $m^2 - 1 \equiv 0 \pmod 8$ and likewise $p_i^2 - 1 \equiv 0 \pmod 8, 1 \leq i \leq r$. It follows that the product of two or more factors in the above summation is divisible by 64, hence

$$m^2 - 1 \equiv \sum_{i=1}^{r} (p_i^2 - 1) \pmod{64}.$$

Moreover each term is divisible by 8, so

$$\frac{m^2-1}{8} \equiv \sum_{i=1}^{r} \frac{p_i^2-1}{8} \pmod 8,$$

as integers. It follows that

$$(-1)^{\frac{m^2-1}{8}} = (-1)^{\sum_{i=1}^r \frac{p_i^2-1}{8}} = \prod_{i=1}^{r} (-1)^{\frac{p_i^2-1}{8}} = \prod_{i=1}^{r} \left(\frac{2}{p_i}\right) = \left(\frac{2}{m}\right).$$

The last part of the theorem, in the case $m, n > 1$ and $(m, n) = 1$, is equivalent to

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

But

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{\substack{1\le i\le r\\ 1\le j\le s}} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) \overset{\text{Thm 11.10}}{=} \prod_{\substack{1\le i\le r\\ 1\le j\le s}} (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = (-1)^t$$

where

$$t = \sum_{\substack{1\le i\le r\\ 1\le j\le s}} \frac{p_i-1}{2}\cdot\frac{q_j-1}{2} = \sum_{1\le i\le r} \frac{p_i-1}{2} \sum_{1\le j\le s} \frac{q_j-1}{2}.$$

By (11.8), we have $t \equiv \dfrac{m-1}{2}\cdot\dfrac{n-1}{2} \pmod 2$ and the quadratic reciprocity law follows. □

Jacobi symbols have many applications aside from their use in understanding the reciprocity step formulated by Euler. The following result is an example of how they can be used in the study of certain Diophantine equations.

Proposition 11.15. *The Diophantine equation*

$$y^2 = x^3 + k$$

has no solution if $k = (4n-1)^3 - 4m^2$ *and no prime* $p \equiv 3 \pmod 4$ *divides* m.

Proof. We argue by contradiction. Assume that (x, y) is a solution. Since $k \equiv -1 \pmod 4$, it follows that

$$y^2 \equiv x^3 - 1 \pmod 4.$$

But $y^2 \equiv 0, 1 \pmod 4$, so x cannot be even and $x \not\equiv -1 \pmod 4$. Therefore $x \equiv 1 \pmod 4$.

Let $a = 4n - 1$. Then $a \equiv -1 \pmod 4$ and $k = a^3 - 4m^2$. We have

$$y^2 = x^3 + k = x^3 + a^3 - 4m^2,$$

so

$$y^2 + 4m^2 = x^3 + a^3 = (x + a)(x^2 - ax + a^2). \tag{11.9}$$

Given that $x \equiv 1 \pmod 4$ and $a \equiv -1 \pmod 4$, we have that the last factor

$$x^2 - ax + a^2 \equiv 3 \pmod 4.$$

Thus $x^2 - ax + a^2$ is odd and it must have some prime divisor $p \equiv 3 \pmod 4$. But (11.9) implies that $p \mid y^2 + 4m^2$, i.e. $-4m^2 \equiv y^2 \pmod p$ so

$$\left(\frac{-4m^2}{p}\right) = 1.$$

On the other hand, since $p \equiv 3 \pmod 4$, we have that $p \nmid m$ and therefore

$$\left(\frac{-4m^2}{p}\right) = \left(\frac{-1}{p}\right) = -1 \text{ (contradiction!)}$$

□

We now go back to our main goal of understanding the reciprocity step in Euler's strategy. For that we need the following property of the Jacobi symbol.

Proposition 11.16. *If m, n are positive odd integers and is an integer with $D \equiv 0, 1 \pmod 4$ such that $m \equiv n \pmod D$, then*

$$\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right).$$

Proof. First we treat the case when $D \equiv 1 \pmod 4$.

If $D > 0,$ then

$$\left(\frac{D}{m}\right) = (-1)^{\frac{m-1}{2}\frac{D-1}{2}}\left(\frac{m}{D}\right).$$

But $\frac{D-1}{2}$ is even, hence $\left(\frac{D}{m}\right) = \left(\frac{m}{D}\right)$. The argument holds for any positive odd integer m, and it can therefore be applied just as well to n. The result follows immediately since $m \equiv n \pmod D$.

If $D < 0,$ set $d = -D$. Then $d > 0$ and $d \equiv 3 \pmod 4$, so $\frac{d+1}{2}$ is even. We have

$$\left(\frac{D}{m}\right) = \left(\frac{-d}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{d}{m}\right) = (-1)^{\frac{m-1}{2}}(-1)^{\frac{m-1}{2}\frac{d-1}{2}}\left(\frac{m}{d}\right) = (-1)^{\frac{m-1}{2}\frac{d+1}{2}}\left(\frac{m}{d}\right) = \left(\frac{m}{d}\right).$$

Since the same holds for n, the result follows from the fact that $m \equiv n \pmod d$.

Now consider the other case, $D \equiv 0 \pmod 4$. It follows that $D = 2^a b$ for some positive odd integer b and $a \geq 2$.

If $D > 0$, then

$$\left(\frac{D}{m}\right) = \left(\frac{2}{m}\right)^a \left(\frac{b}{m}\right) = (-1)^{\frac{m^2-1}{8}a}(-1)^{\frac{m-1}{2}\frac{b-1}{2}}\left(\frac{m}{b}\right).$$

Similarly,

$$\left(\frac{D}{n}\right) = (-1)^{\frac{n^2-1}{8}a}(-1)^{\frac{n-1}{2}\frac{b-1}{2}}\left(\frac{n}{b}\right).$$

The result would follow if we showed that

$$\frac{m^2-1}{8}a \equiv \frac{n^2-1}{8}a \pmod 2 \tag{11.10}$$

and

$$\frac{m-1}{2}\frac{b-1}{2} \equiv \frac{n-1}{2}\frac{b-1}{2} \pmod 2. \tag{11.11}$$

We have

$$\frac{m-1}{2}\frac{b-1}{2} - \frac{n-1}{2}\frac{b-1}{2} = \frac{m-n}{2}\frac{b-1}{2}$$

and this is even since $4 \mid m-n$. Thus (11.11) is proved. For the other relation, we have

$$\frac{m^2-1}{8}a - \frac{n^2-1}{8}a = \frac{m^2-n^2}{8}a = \frac{(m-n)(m+n)}{8}a.$$

Now $2 \mid m+n$ and $2^a \mid m-n$. Thus $m^2 - n^2 \equiv 0 \pmod{16}$ when $a \geq 3$ and (11.10) follows in this case. On the other hand, if $a = 2$, then $\frac{m^2-n^2}{8}a$ is again even and we are done. (We used the fact that $\frac{m^2-n^2}{8} \in \mathbb{Z}$.)

If $D < 0$, set $d = -D$. Then $d > 0$ and $d \equiv 0 \pmod 4$. From above it follows that

$$\left(\frac{d}{m}\right) = \left(\frac{d}{n}\right).$$

We also have

$$\left(\frac{D}{m}\right) = \left(\frac{-d}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{d}{m}\right) = (-1)^{\frac{m-1}{2}}\left(\frac{d}{m}\right)$$

and, similarly,

$$\left(\frac{D}{n}\right) = (-1)^{\frac{n-1}{2}}\left(\frac{d}{n}\right).$$

The result follows from the fact that

$$\frac{m-1}{2} \equiv \frac{n-1}{2} \pmod 2 \iff 2 \mid \frac{m-n}{2} \iff 4 \mid m-n \Leftarrow \begin{cases} m \equiv n \pmod D \\ D \equiv 0 \pmod 4. \end{cases}$$

□

Theorem 11.17. *Let $D \equiv 0, 1 \pmod 4$ be a nonzero integer. Then there exists a* unique *group homomorphism $\chi_D : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ such that*

$$\chi_D([p]) = \left(\frac{D}{p}\right) \text{ (the Legendre symbol modulo } p\text{) for all odd primes } p \nmid D.$$

Furthermore,

$$\chi_D([-1]) = \begin{cases} 1 & \text{if } D > 0; \\ -1 & \text{if } D < 0. \end{cases}$$

Proof. First we show existence. Let

$$\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\},\ \chi([a]) = \left(\frac{D}{m}\right) \text{ where } m \equiv a \pmod D \text{ is an odd positive integer.}$$

We need to show that this is a well-defined map, and for that we need to prove the following two facts.

Claim 1 For any $(a, D) = 1$ there exists a positive odd integer $m \equiv a \pmod D$.
Claim 2 If m, n are positive odd integers and $m \equiv n \pmod D$, then

$$\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right).$$

The second claim is an immediate consequence of Proposition 11.16. The first one, is also easy. There exists some integer k for which $a + kD > 0$. If D is even, then a has to be odd and $a + kD$ is odd and positive. If D is odd, then either $a + kD$ or $a + kD + |D|$ is both odd and positive.
The map χ is clearly a group homomorphism since the Jacobi symbol is completely multiplicative. The condition on primes is just as clear.

Now we have to prove uniqueness. Assume that $f : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ is a group homomorphism with $f([p]) = \left(\frac{D}{p}\right)$ for any odd prime $p \nmid D$. Clearly $f(m) = 1$. Also, for any odd integer $m > 1$, we have $m = p_1 \cdots p_r$ for some odd primes $p_1, \ldots, p_r$. Then

$$f([m]) = f([p_1]) \cdots f([p_r]) = \left(\frac{D}{p_1}\right) \cdots \left(\frac{D}{p_r}\right) = \left(\frac{D}{m}\right) = \chi([m]).$$

Since we have shown that every class $[a] \in (\mathbb{Z}/D\mathbb{Z})^\times$ contains a positive odd integer m, it follows that $f([a]) = \chi([a])$ for all $[a] \in (\mathbb{Z}/D\mathbb{Z})^\times$.
The proof for the expression of $\chi_D([-1])$ is left as an exercise.

□

Corollary 11.18. *Let n be a nonzero integer and let $\chi = \chi_{-4n} : (\mathbb{Z}/4n\mathbb{Z})^\times \to \{\pm 1\}$ be the group homomorphism defined in Theorem 11.17 when $D = -4n$. Let p be an odd prime, $p \nmid n$. The following are equivalent.*

(i) $p \mid a^2 + nb^2$ *for some integers* $(a, b) = 1$.

(ii) $\left(\dfrac{-n}{p}\right) = 1$.

(iii) $[p] \in \ker \chi \subset (\mathbb{Z}/4n\mathbb{Z})^\times$.

Proof. The statements (i) and (ii) are equivalent by Proposition 11.2.
We want to show that $(ii) \iff (iii)$. Theorem 11.17 says that $(iii) \iff \left(\dfrac{-4n}{p}\right) = 1$. Since

$$\left(\frac{-4n}{p}\right) = \left(\frac{2}{p}\right)^2 \left(\frac{-n}{p}\right) = \left(\frac{-n}{p}\right),$$

the proof is complete. □

Note that this finishes the Reciprocity Step from Euler's strategy because if $\ker(\chi) = \{[\alpha], [\beta], [\gamma], \ldots\}$, Corollary 11.18 says that

$$p \mid a^2 + nb^2, (a, b) = 1 \iff p \equiv \alpha, \beta, \gamma, \ldots \pmod{4n}.$$

This is precisely the kind of condition we were looking for.