Math 104B: Number Theory II (Winter 2012)

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 Multiplicative functions

A function $f : \mathbb{Z} \to \mathbb{C}$ is *multiplicative* if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$. It is *completely multiplicative* if $f(mn) = f(m)f(n)$ for all integers m, n regardless of their gcd.

Fact: If f is a multiplicative function than so is $g : \mathbb{Z} \to \mathbb{C}$ defined by

$$g(n) = \sum_{d|n} f(d).$$

Examples of multiplicative, but not completely multiplicative functions:

- $d(n) =$ the number of divisors of n (divisor function)
- $\sigma(n) =$ the sum of the divisors of n
- $\phi(n) =$ the number of positive integers $< n$ and relatively prime to n (Euler's ϕ function)

Assume that we know that $f(n)$ is a multiplicative function. Then in order to be able to evaluate it at any positive integer, it is enough to know its value at prime powers. That is because

$$f(p_1^{a_1} \dots p_r^{a_r}) = f(p_1^{a_1}) \dots f(p_r^{a_r})$$

for any distinct primes $p_1, \dots, p_r$. We can take advantage of this feature to deduce formulas for various multiplicative functions. For instance, for $n = p_1^{a_1} \dots p_r^{a_r}$,

- $d(n) = (a_1 + 1) \dots (a_r + 1)$
- $\sigma(n) = \dfrac{p_1^{a_1} - 1}{p_1 - 1} \cdots \dfrac{p_r^{a_r} - 1}{p_r - 1}$
- $\phi(n) = p_1^{a_1 - 1}(p_1 - 1) \dots p_r^{a_r - 1}(p_r - 1) = n \left(1 - \dfrac{1}{p_1}\right) \dots \left(1 - \dfrac{1}{p_r}\right).$

1.4 Linear diophantine equations

These are equations of the form

$$a_1 x_1 + \ldots + a_k x_k = c$$

with *integer* coefficients and for which we want to find *integer solutions*. We know that such solutions exist if and only if the gcd of the coefficients $a_1, \dots, a_n$ divides c.

1.5 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 $\pmod{m_1 \ldots m_r}$.

2 Primes as sums of squares

Our goal in the next couple of lectures is to prove the following result formulated by Fermat.

Theorem 2.1. *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.)

2.1 Reciprocity step

The reciprocity step follows immediately from the following result.

Lemma 2.2. *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.

□

2.2 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 2.3. *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 $N=a^2+b^2$ 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 2.3, 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 2.1.

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 $x^2 + y^2 \not\equiv 0 \pmod 3$.

3 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

$$x^2 + y^2 = z^2. \tag{3.1}$$

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 that, 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 $u \not\equiv v \pmod 2$.

4 More descent

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

$$x^4 + y^4 = z^4. \tag{4.1}$$

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 (4.1). 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 (4.1). 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

$$X^4 + Y^4 = T^2. \tag{4.2}$$

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 3) 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 3, 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 (4.2) 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 (4.2) 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 (4.1) led to a contradiction, and that proves that no such solution can exist.

5 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 $(x_1, y_1, z_1) = 1$.

6 Fermat-Pell equations

We will consider equations of the form

$$x^2 - dy^2 = 1 \tag{6.1}$$

and

$$x^2 - dy^2 = -1. \tag{6.2}$$

We want to figure out for which d they have (non-trivial) integer solutions. 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 6.1. *Let d be a positive integer.*

1. *If the equation*
$$x^2 - dy^2 = 1 \tag{6.1}$$
has one positive solution, then it has infinitely many positive solutions.

2. *If the equation*
$$x^2 - dy^2 = -1 \tag{6.2}$$
has one positive solution, then both (6.1) *and* (6.2) *have infinitely many positive solutions.*

The theorem follows immediately from the following lemma.

Lemma 6.2. *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 not a square.

6.1 Diophantine approximation

We want to figure out when these equations have solutions. We will deal first with the equation (6.1), namely

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

Example 1 The smallest positive solution to $x^2 - 61y^2 = 1$ is $(1766319049, 226153980)$.

Example 2 The smallest positive solution to $x^2 - 21y^2 = 1$ is $(55, 12)$.

Example 3 The smallest positive solution to $x^2 - 58y^2 = 1$ is $(19603, 2574)$.

If (x, y) is a positive integer solution to Pell's equation (6.1), then we must have

$$(x + y\sqrt{d}\,)(x - y\sqrt{d}\,) = 1 \iff x - y\sqrt{d} = \frac{1}{x + y\sqrt{d}} \tag{6.3}$$

If x, y are positive integers, the quantity $x + y\sqrt{d}$ will be relatively large. Hence $x - y\sqrt{d}$ must be a small positive real number. So, if we can find x, y positive integers such that $x - y\sqrt{d}$ is as small as possible, then the product $(x + y\sqrt{d}\,)(x - y\sqrt{d}\,)$ has to be a relatively small positive integer. And a small positive integer has a good chance of being equal to 1, or at least close to it. That chance increases if we can keep the size of our large factor $x + y\sqrt{d}$ under control.

We start by investigating the question of how small we can make $x - y\sqrt{d}$ and we will follow Dirichlet's answer to this question.

For any integer $y > 0$ we can choose x to be the closest integer to $y\sqrt{d}$ and this ensures that $\left|x - y\sqrt{d}\right| \leq \frac{1}{2}$. But we can do much better than that.

Example Take $d = 13$.

$$\begin{array}{llll} y = 1 & x = 4 & \implies & \left|x - y\sqrt{13}\right| \sim 0.3944 \\ y = 5 & x = 18 & \implies & \left|x - y\sqrt{13}\right| \sim 0.0277 \end{array}$$

Dirichlet employed a simple, yet very powerful, idea to answer the question of how small $\left|x - y\sqrt{d}\right|$ can become: the **pigeonhole principle.** This principle simply says that if there more pigeons than pigeonholes, then at least one of pigeonholes contains more than one pigeon.

Theorem 6.3 (Dirichlet's diophantine approximation theorem)**.** *Let $\alpha \in \mathbb{R}_{>0} \setminus \mathbb{Q}$ be a positive irrational number. Then there are infinitely many pairs of positive integers (x, y) such that*

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

Proof. Pick a large integer $T > 0$. For $0 \leq t \leq T$ write each of the numbers

$t\alpha = N_t + F_j t$ where $N_t = \lfloor j\alpha \rfloor$ is the floor of $j\alpha$ and $F_t \in [0, 1)$ is the fractional part of $j\alpha$.

Our pigeons are the $T + 1$ numbers $F_0, F_1, \ldots, F_T$.
Our pigeonholes are the T subintervals of $[0, 1)$ given by $\left[\frac{t-1}{T}, \frac{t}{T}\right), 1 \leq t \leq T$.
The pigeonhole principle ensures that there exist

$$0 \leq j < k \leq T \text{ such that } |F_k - F_j| < \frac{1}{T}.$$

But $F_j = j\alpha - N_j$ and $F_k = k\alpha - N_k$. Substituting above, we get

$$|(N_k - N_j) - (k - j)\alpha| < \frac{1}{T}$$

Set $x = N_k - Nj$ and $y = k - j$. Then $x, y \in \mathbb{Z}_{>0}$ and $|x - y\alpha| < \frac{1}{T}$. On the other hand, since $0 \leq j < k \leq T$ it follows that $0 < y = k - j \leq T$.
To recap we have that

$$0 < y \leq T \tag{6.4}$$

and

$$|x - y\alpha| < \frac{1}{T}. \tag{6.5}$$

Note that by taking T larger and larger we automatically get new pairs of positive integers (x, y) that satisfy (6.4) and (6.5). This happens because $|x - y\alpha| > 0$ (recall that $\alpha \notin \mathbb{Q}$!). For any fixed pair of positive integers (x_0, y_0) we can make T large enough so that (6.5) does not hold anymore. Therefore we obtain another pair of positive integers (x_1, y_1) for this new T.

Continuing the procedure and making T larger and larger yields infinitely many pairs of positive integers that satisfy (6.4) and (6.5). Note also that (6.4) implies that

$$\frac{1}{T} \leq \frac{1}{y},$$

and our proof is complete. □

Going back to Pell's equation (6.1), we will apply Dirichlet's theorem to $\alpha = \sqrt{d}$. The fact that $d > 0$ is not a square ensures that $\sqrt{d} \notin \mathbb{Q}$. Hence there are infinitely many pairs of positive integers (x, y) such that $|x - y\sqrt{d}| < 1/y$. We would like the left hand side here to be equal to $|x + y\sqrt{d}|$ since that would yield a solution to Pell's equation.

Idea: take two pairs (x, y) for which $x^2 - dy^2$ gives the same value and "divide" them. Let's see on an example what we mean.

Example $d = 13$

$$\begin{aligned} (x_1, y_1) = (11, 3) \quad &\Longrightarrow \quad x_1^2 - 13y_1^2 = 4 \\ (x_1, y_1) = (119, 33) \quad &\Longrightarrow \quad x_2^2 - 13y_2^2 = 4 \end{aligned}$$

We "divide" by taking the quotient

$$\frac{x_2 - y_2\sqrt{d}}{x_1 - y_1\sqrt{d}} = \frac{119 - 33\sqrt{13}}{11 - 3\sqrt{13}} = \frac{119 - 33\sqrt{13}}{11 - 3\sqrt{13}} \cdot \frac{11 + 3\sqrt{13}}{11 + 3\sqrt{13}} = \frac{11}{2} - \frac{3}{2}\sqrt{13}.$$

We still don't have what we want because $11/2$ and $3/2$ are not integers. Let's try again with another pair (x_3, y_3). Namely,

$$(x_3, y_3) = (14159, 3927) \quad \Longrightarrow \quad x_3^2 - 13y_3^2 = 4.$$

Then

$$\frac{x_3 - y_3\sqrt{d}}{x_1 - y_1\sqrt{d}} = \frac{14159 - 3927\sqrt{13}}{11 - 3\sqrt{13}} = 649 - 180\sqrt{13}.$$

The key point here is that $(x_1, y_1) \equiv (x_3, y_3) \pmod 4$, but $(x_1, y_1) \not\equiv (x_2, y_2) \pmod 4$.

Lemma 6.4. *Let d be an integer that is not a perfect square. Set*

$$F_d = \{x + y\sqrt{d}; x, y \in \mathbb{Q}\} \subset \mathbb{C}$$

and

$$R_d = \{m + n\sqrt{d}; m, n \in \mathbb{Z}\} \subset F_d.$$

(i) *If* $x, y \in \mathbb{Q}$, *then* $x + y\sqrt{d} = 0 \iff x = y = 0$.

(ii) $\mathbb{Z} \subset R_d, \mathbb{Q} \subset F_d$.

(iii) $z_1, z_2 \in R_d \implies z_1 \pm z_2, z_1 z_2 \in R_d$.

(iv) $z_1, z_2 \in F_d \implies z_1 \pm z_2, z_1 z_2 \in F_d$.

(v) $z \in F_d, z \neq 0 \implies \dfrac{1}{z} \in F_d$.

Proof. Exercise. □

Lemma 6.5. *With the same notation as in Lemma 6.4, if* $(x + y\sqrt{d})^n = A + B\sqrt{d}$ *with* $x, y, A, B \in \mathbb{Z}$ *and* $n \in N$, *then* $(x - y\sqrt{d})^n = A - B\sqrt{d}$. *Same statement for* $x, y, A, B \in \mathbb{Q}$.

Proof. Induction on n. □

Theorem 6.6. *Let* d *be a positive integer that is not a perfect square.*

(i) *Then Pell's equation*

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

always has positive integer solutions.

(ii) *Moreover, let* (a_1, b_1) *be the positive integer solution with the smallest* a_1 *and set*

$$z = a_1 + b_1\sqrt{d}.$$

(Alternatively, we could choose the pair that gives the smallest $z > 1$.*)*
Define (a_k, b_k) *to be the positive integers given by the formula*

$$a_k + b_k\sqrt{d} = z^k = (a_1 + b_1\sqrt{d})^k \quad \forall k \geq 1. \tag{6.6}$$

Then $(a_k, b_k), k \geq 1$, *are all the positive integer solutions to Pell's equation.*

Proof. To prove the first part we will employ again the pigeonhole principle. Dirichlet's Theorem 6.3 implies that there are infinitely many pairs (x, y) of positive integers such that $\left|x - y\sqrt{d}\right| < \dfrac{1}{y}$.

For any such (x, y) we have $0 < x < y\sqrt{d} + \dfrac{1}{y}$, and so

$$x + y\sqrt{d} < 2\sqrt{d} + \frac{1}{y} < 3y\sqrt{d}.$$

Therefore

$$\left|x^2 - y^2 d\right| = \left|x - y\sqrt{d}\right| \left|x + y\sqrt{d}\right| < \frac{1}{y} \cdot 3y\sqrt{d} = 3\sqrt{d}. \tag{6.7}$$

Let $T = \lfloor 3\sqrt{d} \rfloor$. We will apply the pigeonhole principle to

pigeons: pairs of positive integers (x, y) such that $\left|x - y\sqrt{d}\right| < \dfrac{1}{y}$. There are infinitely many pigeons (cf. Theorem 6.3).

pigeonholes: integers $-T \le m \le T$. There are $2T + 1$ pigeonholes.

Since we have infinitely many pigeons and only finitely many pigeonholes, it follows that at least one pigeonhole must contain infinitely many pigeons. Therefore there exist an integer M such that $|M| < 3\sqrt{d}$ and an infinite sequence (x_k, y_k) such that

$$x_k < x_{k+1}, \quad y_k < y_{k+1}, \quad x_k^2 - y_k^2 d = M. \tag{6.8}$$

We would like to "divide" two such pairs to get a solution to Pell's equation. But as we've seen in our example, we need to choose our pairs carefully. We do that by employing the pigeonhole principle again. This time the protagonists are:

pigeons the infinitely many pairs of positive integers (x_k, y_k);

pigeonholes pairs of integers (A, B) with $0 \le A, B \le M - 1$. There are M^2 pigeonholes.

Once again, we have infinitely many pigeons and finitely many pigeonholes. It follows that there are two different pairs (x_k, y_k) and (x_j, y_j) with $k < j$ and

$$x_k \equiv x_j \pmod{M}, \quad y_k \equiv y_j \pmod{M}.$$

Then, by (6.8),

$$\frac{x_j - y_j\sqrt{d}}{x_k - y_k\sqrt{d}} = \frac{x_j - y_j\sqrt{d}}{x_k - y_k\sqrt{d}} \cdot \frac{x_k + y_k\sqrt{d}}{x_k + y_k\sqrt{d}} = \frac{(x_j x_k - d y_j y_k) + (x_j y_k - x_k y_j)\sqrt{d}}{M}.$$

Set

$$x = \frac{x_j x_k - d y_j y_k}{M} \quad y = \frac{x_j y_k - x_k y_j}{M}.$$

First we see that

$$x^2 - y^2 d = \frac{(x_j^2 - y_j^2 d)(x_k^2 - y_k^2 d)}{M^2} = 1.$$

Then we use the congruence relations to show that x, y are integers. Indeed,

$$x_j x_k - d y_j y_k \equiv x_k^2 - d y_k^2 \pmod{M} \equiv 0 \pmod{M}$$

and

$$x_j y_k - x_k y_j \equiv x_k y_k - x_k y_k \pmod{M} \equiv 0 \pmod{M}.$$

Changing signs if necessary, we found a nonnegative integers x, y such that $x^2 - y^2 d = 1$. Clearly this implies that $x \ge 1$. We want to show that $y \ne 0$. We argue by contradiction.

Assume $y = 0$. Then

$$x_j y_k = x_k y_j$$

which implies that

$$y_k^2 M = y_k^2(x_j^2 - dy_j^2) = x_k^2 y_j^2 - dy_k^2 y_j^2 = My_j^2.$$

We obtain $y_k = y_j$ which is a contradiction. Therefore $y > 0$ and we found our solution.

Now for the second statement of the theorem. First we should note that $z > 1$ since $a_1, b_1 \geq 1$ and that Lemma 6.4 ensures that a_k, b_k are well defined (i.e. z^k can be indeed written as integer + and integer multiple of $\sqrt{d}$; positivity I leave to you). The same lemma ensures that we do not have any repeat pairs among the (a_k, b_k)'s.

We should also note that

$$z(a_1 - b_1\sqrt{d}) = (a_1 + b_1\sqrt{d})(a_1 - b_1\sqrt{d}) = a_1^2 - db_1^2 = 1,$$

so

$$\frac{1}{z} = a_1 - b_1\sqrt{d}.$$

By Lemma 6.5,

$$z^{-k} = a_k - b_k\sqrt{d} \quad \forall k \geq 1.$$

Thus

$$a_k^2 - b_k^2 d = (a_k + b_k\sqrt{d})(a_k - b_k\sqrt{d}) = z^k \cdot z^{-k} = 1 \quad \forall k \geq 1,$$

which is to say (a_k, b_k) is a solution of the Pell equation (6.1).

And now we have to show that there are no other positive integer solutions. Assume (u, v) is a positive integer solution. We want to show that there exist a positive integer k such that $(u, v) = (a_k, b_k)$.
Let $r = u + v\sqrt{d}$. Then $u \geq a_1 > 0$ and this implies in turn that $v^2 = \frac{u^2-1}{d} \geq \frac{a_1^2-1}{d} = b_1^2$. Since we are dealing with positive numbers, this implies $v \geq b_1$, so $r \geq z > 1$.

It follows that there exist an integer $k \geq 1$ such that $z^k \leq r < z^{k+1}$. Then $1 \leq z^{-k}r < z$, which can be rewritten as

$$1 \leq (a_k - b_k\sqrt{d})(u + v\sqrt{d}) < z.$$

Hence

$$1 \leq s + t\sqrt{d} < z. \tag{6.9}$$

where

$$s = a_k u - b_k v d \quad \text{and} \quad t = a_k v - b_k u.$$

Moreover,

$$s^2 - t^2 d = (a_k u - b_k v d)^2 - d(a_k v - b_k u)^2 = (a_k^2 - db_k^2)(u^2 - dv^2) = 1 \tag{6.10}$$

We need to show that $s + t\sqrt{d} = z^{-k}r \stackrel{?}{=} 1$. We do that by excluding all other possibilities.

Assume $s < 0, t < 0$. Then $s + t\sqrt{d} < 0$ which contradicts (6.9).

Assume $s < 0, t \geq 0$. Then $-s + \sqrt{d} > s + t\sqrt{d} \geq 1$ and thus

$$-1 = -s^2 + t^2 d = (-s + t\sqrt{d})(s + t\sqrt{d}) \geq 1 \cdot 1 \text{ (contradiction).}$$

Assume $s \geq 0, t < 0$. Then $s - t\sqrt{d} > s + t\sqrt{d} \geq 1$ and thus

$$1 = s^2 - t^2 d = (s - t\sqrt{d})(s + t\sqrt{d}) \geq s - t\sqrt{d} > 1 \text{ (contradiction).}$$

Assume $s > 0, t > 0$. Then $s \geq a_1 > 0$ since (a_1, b_1) is the positive integer solution with the smallest a_1. By (6.10) we have

$$t^2 = \frac{s^2 - 1}{d} \geq \frac{a_1^2 - 1}{d} = b_1^2.$$

Again we are dealing with positive integers, so $t \geq b_1$ and $s + t\sqrt{d} \geq a_1 + b_1\sqrt{d} = z$ which contradicts (6.9).

Assume $s = 0$. Then $t^2 d = -1$ which is impossible since $d > 0$.

The only possibility left is that $t = 0$. This implies $s = 1$, hence $z^k = r$. □

6.2 Continued fractions

We still want a method for finding that smallest solution to Pell's equation (6.1). 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 A one computes its continued fraction expansion as follows.

$$\begin{aligned} x_0 &= A, & a_0 &= \lfloor x_0 \rfloor \\ x_{i+1} &= \frac{1}{x_i - a_i}, & a_{i+1} &= \lfloor x_{i+1} \rfloor \quad \forall i \geq 0 \end{aligned} \tag{6.11}$$

This formula ensures that $x_i, a_i \geq 1$ 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 A, where the a_i's are computed according to the procedure given in (6.11).

Example 6.7.

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

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

Example 6.8. 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 (6.11) 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 6.9. The continued fraction of $\sqrt{2}$ is $[1, 2, 2, 2, 2, \ldots]$.

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

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

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

Example 6.10.

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

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

We can continue this procedure and see that in general

$$\begin{aligned} p_{n+1} &= a_{n+1} p_n + p_{n-1} \quad \text{for all } n \geq 1, \quad p_0 = a_0, \qquad p_1 = a_0 a_1 + 1; \\ q_{n+1} &= a_{n+1} q_n + q_{n-1} \quad \text{for all } n \geq 1, \quad q_0 = 1, \qquad q_1 = a_1. \end{aligned} \tag{6.12}$$

Note that

$$p_1 q_0 - p_0 q_1 = a_0 a_1 + 1 - a_0 a_1 = 1.$$

Furthermore, (6.12) implies that

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

It follows by induction that

$$p_{n+1} q_n - p_n q_{n+1} = (-1)^n \quad \forall n \geq 0. \tag{6.13}$$

In particular, p_n, q_n are relatively prime for all n and therefore the convergents $\frac{p_n}{q_n}$ are indeed written in lowest terms with p_n, q_n computed using the recurrence relations (6.12).

Moreover, if $[a_0, a_1, \ldots]$ is an infinite continued fraction (6.12) implies that the denominators q_n keep growing, while (6.13) tells us that $\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} = \frac{(-1)^n}{q_n q_{n+1}}$. Therefore the convergents $\frac{p_n}{q_n}, n \geq 0$, form a Cauchy sequence. We can now make the following definition.

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

Theorem 6.11. *If* $A \in \mathbb{R} \setminus \mathbb{Q}$, *then the continued fraction expansion of* A *is infinite and* A *is indeed equal to its continued fraction obtained according to* (6.11), *i.e.*

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

Proof. Exercise. □

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

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

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

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

Examples

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

Example 6.12. Let $A = [a, \bar{b}]$. Note that our procedure (6.11) ensures that $b \geq 1$. Then

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

On the other hand,

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

so

$$B^2 = bB + 1.$$

Since $B > 0$, the quadratic formula tells us that

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

and therefore

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

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

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

We have already seen this for $a = 1$, namely we have seen that $\sqrt{2} = [1, \bar{2}]$.

Lemma 6.13. *If $B = [\overline{b_1, \ldots, b_m}]$ has a purely periodic continued fraction with, then there are positive integers x, y, u, v such that*

$$B = \frac{xB + y}{uB + v}.$$

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

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

The rest is just algebraic manipulation. □

Theorem 6.14. *(i) If the continued fraction expansion of a real number A is periodic, i.e.*

$$A = [a_0, \ldots, a_k, \overline{b_0, b_1, \ldots, b_m}],$$

then there exist integers r, s, t, d with $d > 0$ not a square, $s, t \neq 0$ such that

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

(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

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

is periodic.

Proof. For the first part, denote $B = [\overline{b_0, b_1, \ldots, b_m}]$. Lemma 6.13 implies that B satisfies a quadratic equation

$$aB^2 + bB + c = 0.$$

Note that the discriminant $\Delta = b^2 - 4ac > 0$ since $B \in \mathbb{R} \setminus \mathbb{Q}$. (This is because B 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, B is of the form

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

for some integers r', s', t'. In particular $B \in F_d$ and since F_d is closed under addition, division and multiplication, it follows that $A \in F_d$, so A is of the desired form.

The argument for the second part is more complicated. First observe that

$$A = \frac{p_0 + \sqrt{D}}{q_0}$$

for some integers $D > 0, p_0, q_0$ and that we can choose them so that $q_0 \mid p_0^2 - D$. (In order to see this, you might want to take advantage of the fact that A is the root of some quadratic equation with integer coefficients.) The procedure (6.11) for computing the continued fraction of A is the following. Let

$$x_0 = A, a_0 = \lfloor x_0 \rfloor.$$

Next, we set

$$x_1 = \frac{1}{x_0 - \lfloor x_0 \rfloor} \geq 1 \text{ and } a_1 = \lfloor x_1 \rfloor.$$

Then at each step we set

$$x_{i+1} = \frac{1}{x_i - \lfloor x_i \rfloor} > 1 \text{ and } a_{i+1} = \lfloor x_{i+1} \rfloor \geq 1.$$

The statement of the second part of the theorem is equivalent to showing that there exist positive integers m, k such that $x_k = x_{k+m}$. (In this case, the continued fraction procedure ensures that $a_k = a_{m+k}$ and $x_{k+1} = x_{m+k+1}$, etc. . .)

We have

$$x_1 = \frac{1}{\frac{p_0+\sqrt{D}}{q_0} - a_0} = \frac{q_0}{p_0 - a_0 q_0 + \sqrt{D}} = \frac{q_0(p_0 - a_0 q_0 + \sqrt{D})}{p_0^2 - D + q_0(a_0^2 q_0 - 2a_0 p_0)}.$$

Since $q_0 \mid p_0^2 - D$ it follows that $p_1 = p_0 - a_0 q_0$ and $q_1 = \frac{p_0^2 - D}{q_0} + a_0^2 q_0 - 2a_0 p_0$ are integers and $x_1 = \dfrac{p_1 + \sqrt{D}}{q_1}$.

Note that $q_1 = \frac{p_1^2 - D}{q_0}$, hence $q_1 \mid p_1^2 - D$.

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

- $1 < x_i = \dfrac{p_i + \sqrt{D}}{q_i}$
- $p_{i+1} = p_i - a_i q_i \in \mathbb{Z}$
- $q_{i+1} = \dfrac{p_{i+1}^2 - D}{q_i} \in \mathbb{Z}$

- $q_i \mid p_i^2 - D$
- $q_i \neq 0$ (this comes down to $\sqrt{D} \notin \mathbb{Q}$.)
- $q_i > 0$
- $0 < p_i - \sqrt{D} < q_i < p_i + \sqrt{D} < 2\sqrt{D}$.

It follows that (p_i, q_i) must be positive integers smaller than $2\sqrt{D}$. There are only finitely many possibilities for such pairs, and thus, the pigeonhole principle ensures that there are positive integers m, k such that $(p_k, q_k) = (p_{m+k}, q_{m+k})$ and so $x_k = x_{m+k}$. □

Going back to our initial goal, the study of Pell's equations, we can now formulate the following results. We state them without proofs, which you can find in any standard textbook. One of my favorites is Davenport's *Higher Arithmetic*.

Theorem 6.15. *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

$$x^2 - dy^2 = 1 \tag{6.1}$$

is given by

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

Theorem 6.16. *Let $d > 0$ not a perfect square. Pell's equation*

$$x^2 - dy^2 = -1 \tag{6.2}$$

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

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

In Section 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 2.3 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 7.1. *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 7.2. *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 2.

Descent step

We start by considering the generalization of the Lemma 2.3. This is the first component of our descent step.

Lemma 7.3. *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 2.3 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

$$p \text{ prime}, p \mid a^2 + nb^2 \text{ with } (a, b) = 1 \implies p = x^2 + ny^2. \tag{7.1}$$

As in the Section 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 2.2.

For $n = 1$: done in Section 2.2.

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

$$x^2 + 2y^2. \tag{7.2}$$

If all the other prime divisors of $a^2 + 2b^2$ could be written in the form (7.2), then Lemma 7.3 would imply that p can also be written as in (7.2) 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 (7.2). 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 (7.2). 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 (7.1) *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. (See Section 9.)

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 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

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

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 8).

8 Quadratic reciprocity

8.1 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 8.1. *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 8.1 would not hold. For instance, if we take $n = 15$ we have 8 modulo classes relatively prime to $15 : 1, 2, 3, 7, 811, 13, 14$. 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 7 is provided by the following fact.

Proposition 8.2. *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 8.3.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4}. \end{cases}$$

Proof. Follows immediately from Proposition 8.2 and Theorem 2.1. □

Lemma 8.4 (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 8.1, there are exactly $\frac{p-1}{2}$ quadratic residues $\pmod{p}$. Hence no quadratic residue can be a root of $f(X)$, and we are done.

□

Proposition 8.5. *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 8.6.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8}. \end{cases}$$

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 8.7.

$$p \mid a^2 + 2b^2 \text{ for some integers } (a,b) = 1 \iff p \equiv 1, 3 \pmod{8}.$$

Proof. By Proposition 8.2 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 7, proves Theorem 7.1.

Lemma 8.8 (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*

$$m = \#\{x_t; x_t > \frac{p}{2}, 1 \le t \le \frac{p-1}{2}\}.$$

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 $0 \le x_t \le p-1$. On the other hand, since $p \nmid n$, p cannot divide any of the integers $n, 2n, 3n, \ldots, \dfrac{p-1}{2}n$. So $x_t \ge 1$ for all $1 \le t \le \dfrac{p-1}{2}$.

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

$$A, C \subset \left\{1, 2, \ldots, \frac{p-1}{2}\right\}. \tag{8.1}$$

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

$$\#A \cup C = m + k = \frac{p-1}{2}. \tag{8.2}$$

Taken together, (8.1) and (8.2) 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

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^m \prod_{1\leq t\leq r} x_t \pmod{p} \equiv (-1)^m \prod_{1\leq t\leq r} tn \pmod{p}.$$

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 8.4).

□

Note that we are interested only in the parity of m. The following result deals with said parity.

Proposition 8.9. *Let n be an integer not divisible by p. With the same notation as in Gauss's Lemma 8.8, we have*

$$m \equiv \left((n-1)\frac{p^2-1}{8} + \sum_{1\leq t\leq \frac{p-1}{2}} \left\lfloor \frac{tn}{p} \right\rfloor\right) \pmod{2}.$$

In particular, if n is odd, then

$$m \equiv \left(\sum_{1\leq t\leq \frac{p-1}{2}} \left\lfloor \frac{tn}{p} \right\rfloor\right) \pmod{2}.$$

Proof. Denote

$$\gamma = \sum_{1\leq t\leq \frac{p-1}{2}} \left\lfloor \frac{tn}{p} \right\rfloor.$$

We will use the same notation from the proof of Gauss's Lemma 8.8. 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

$$x_t = p\left\{ \frac{tn}{p} \right\} = \frac{tn}{p} - \left\lfloor \frac{tn}{p} \right\rfloor. \tag{8.3}$$

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 (8.3) above we get that

$$\alpha + \beta = \left(\sum_{1 \leq t \leq \frac{p-1}{2}} tn \right) - p \left(\sum_{1 \leq t \leq \frac{p-1}{2}} \left\lfloor \frac{tn}{p} \right\rfloor \right) = n\frac{p^2-1}{8} - p\gamma. \tag{8.4}$$

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

$$\alpha - \beta + pm = \frac{p^2-1}{8}. \tag{8.5}$$

Adding up (8.4) and (8.5) yields

$$2\alpha + pm = (n+1)\frac{p^2-1}{8} - p\gamma.$$

When we reduce this $\mod 2$, 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 8.10 (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

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}. \tag{8.6}$$

By Gauss's Lemma 8.8 and Proposition 8.9, 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 (8.6) would follow if we proved that

$$\sum_{1\le t\le \frac{p-1}{2}} \left\lfloor \frac{tq}{p} \right\rfloor + \sum_{1\le s\le \frac{q-1}{2}} \left\lfloor \frac{sp}{q} \right\rfloor = \frac{p-1}{2}\,\frac{q-1}{2}. \tag{8.7}$$

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 (8.7) 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).

$$\begin{aligned}\left(\frac{583}{907}\right) &= \left(\frac{11}{907}\right)\left(\frac{53}{907}\right) = (-1)^{\frac{11-1}{2}\frac{907-1}{2}}\left(\frac{907}{11}\right)(-1)^{\frac{53-1}{2}\frac{907-1}{2}}\left(\frac{907}{53}\right) = -\left(\frac{9}{11}\right)\left(\frac{6}{53}\right)\\ &= -\left(\frac{3}{11}\right)^2\left(\frac{2}{53}\right)\left(\frac{3}{53}\right) = -(-1)^{\frac{(53-1)(53+1)}{8}}(-1)^{\frac{53-1}{2}\frac{3-1}{2}}\left(\frac{53}{3}\right) = \left(\frac{2}{3}\right) = -1\end{aligned}$$

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 8.2 implies the reciprocity step for $n=3$ below.

Proposition 8.11. *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 4, prove Theorem 7.2.

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 8.12. *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 8.10),

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

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. □

8.2 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 $\left(\frac{-}{1}\right) : \mathbb{Z} \to \mathbb{C}$ 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 $\left(\frac{-}{m}\right) : \mathbb{Z} \to \mathbb{C}$ 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 8.13. *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 8.14. *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) $\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{m}{n}\right).$

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

$$\frac{m-1}{2} \equiv \sum_{i=1}^{r} \frac{p_i - 1}{2} \pmod 2, \tag{8.8}$$

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

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{\substack{1\le i\le r\\ 1\le j\le s}} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) \overset{\text{Thm 8.10}}{=} \prod_{\substack{1\le i\le r\\ 1\le j\le s}} (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = (-1)^t$$

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 (8.8), 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 8.15. *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

$$y^2 + 4m^2 = x^3 + a^3 = (x + a)(x^2 - ax + a^2). \tag{8.9}$$

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 (8.9) 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 8.16. *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

$$\frac{m^2-1}{8}a \equiv \frac{n^2-1}{8}a \pmod 2 \tag{8.10}$$

and

$$\frac{m-1}{2}\frac{b-1}{2} \equiv \frac{n-1}{2}\frac{b-1}{2} \pmod 2. \tag{8.11}$$

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 (8.11) 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 (8.10) 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 8.17. *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 8.16. 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 8.18. *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 8.17 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 8.2.
We want to show that $(ii) \iff (iii)$. Theorem 8.17 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 8.18 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.

9 Quadratic forms

We now go back to the descent step for primes of the form $x^2 + ny^2$ with $n > 3$. There are two examples we need to keep in mind. Euler made two conjectures regarding the cases $n = 5$ and $n = 14$. First, let's see what the reciprocity step says.
For $n = 5$, we need to look at congruence classes in $(\mathbb{Z}/20\mathbb{Z})^\times$. We can look at them one by one and, using Corollary 8.18, see that

$$p \mid a^2 + 5b^2, (a, b) = 1 \iff p \equiv 1, 3, 7, 9 \pmod{20}.$$

But here's Euler's conjecture (and of course, he had good numerical evidence for it). We have seen that not all divisors of a number of the form $a^2 + 5b^2$ can be written in the same form, which momentarily derailed our strategy. Indeed, things are more complicated in this case and we need to understand what forms the divisors of $a^2 + 5b^2$ can have.

Conjecture 9.1 (Euler)**.** *If* $p \neq 5$ *is an odd prime, then*

$$\begin{aligned} p = x^2 + 5y^2 &\iff p \equiv 1, 9 \pmod{20} \\ 2p = x^2 + 5y^2 &\iff p \equiv 3, 7 \pmod{20} \end{aligned}$$

The congruence classes break into two groups – $1, 9$ and $3, 7$ – that have very different representability properties. To see what's going on, recall that we have seen that not all divisors of a number of the form $a^2 + 5b^2$ can be written in the same form.
The case $n = 14$ is even more complicated.

Conjecture 9.2 (Euler)**.** *If $p \neq 7$ is an odd prime, then*

$$p = \begin{cases} x^2 + 14y^2 \\ 2x^2 + 7y^2 \end{cases} \iff p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$$
$$3p = x^2 + 5y^2 \iff p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}$$

As in the previous case, the congruence classes modulo 56 that appear above are precisely the ones for which $\left(\frac{-14}{p}\right) = 1$. A new feature is that $x^2 + 14y^2$ and $2x^2 + 7y^2$ appear together. Another question is where the $2p$ in Conjecture 9.1 and $3p$ in Conjecture 9.2 come from. Why are they different multiples of p? Why 2 and 3 appear there, and not, say, 29? Gauss composition explains this phenomenon. What other condition is necessary to ensure $p = x^2 + 14y^2$? This is a much deeper question and the answer involves class field theory which is outside the scope of this class. For now, it should be clear that we need to know more about these quadratic polynomials.

Definition. *An integral binary quadratic form (for short, integral bqf) is a degree 2 homogeneous polynomial in two variables with integer coefficients, i.e. $f(x, y) = ax^2 + bxy + cy^2$, $a, b, c, \in \mathbb{Z}$.*

Note: One can define binary quadratic forms over any commutative ring R. In particular, they can be defined over $\mathbb{Q}$ or $\mathbb{R}$.

Definition. *An integral binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is primitive if $(a, b, c) = 1$.*

Note: Any integral form is an integer multiple of a primitive form.

Definition. *An integer m is represented by a integral bqf $f(x, y)$ if the equation*

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

has an integer solution (x, y). If we can find an integer solution with x, y relatively prime, we say that m is properly represented by $f(x, y)$.

Example 9.3. A bqf $f(x, y) = ax^2 + bxy + cy^2$ properly represents both $a = f(\pm 1, 0)$ and $c = f(0, \pm 1)$.

The question we are trying to answer is which primes p can be (properly) represented by the (primitive) integral bqf $x^2 + ny^2$.

Lemma 9.4. *If m is an integer represented by the bqf $f(x, y)$, then m can be written as $m = d^2 m'$ where $m', d \in \mathbb{Z}$ and m' is properly represented by $f(x, y)$.*

Proof. Since $m = f(x, y)$ for some integers x, y with $d = (x, y)$, it follows that $m = d^2 f(x', y')$ where $x = dx', y = dy'$. But then $(x', y') = 1$ and the result follows by setting $m' = f(x', y')$. □

Definition. *Two bqf's $f(x, y)$ and $g(x, y)$ are equivalent if there are integers $\alpha, \beta, \gamma, \delta$ such that $f(x, y) = g(\alpha x + \beta y, \gamma x + \delta y)$ and $\alpha\delta - \beta\gamma = \pm 1$. In linear algebra terms, this just says that there exists a matrix $A \in \mathrm{GL}(2, \mathbb{Z})$ – the group of 2×2 invertible matrices with coefficients in $\mathbb{Z}$ –such that*

$$f(\vec{x}) = g(A\vec{x})$$

Note: You can think of the bqf $f(x, y) = ax^2 + bxy + cy^2$ as

$$f(\vec{x}) = {}^t\vec{x} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \vec{x}$$

Proposition 9.5. *The above definition describes indeed an equivalence relation.*

Proof. Exercise. □

Definition. *We say that the equivalence of two bqf's is a proper equivalence if $\alpha\delta - \beta\gamma = 1$ (i.e. the matrix $A \in \mathrm{SL}(2, \mathbb{Z})$ – the subgroup of $\mathrm{GL}(2, \mathbb{Z})$ that consists of matrices with determinant equal to 1). It is called an improper equivalence otherwise (i.e. $\alpha\delta - \beta\gamma = -1 \iff \det A = -1$).*

Proposition 9.6. *Proper equivalence is indeed an equivalence relation.*

Proof. Exercise. □

Note: The terms "equivalence" and "proper equivalence" are due to Gauss. He had good reason to distinguish between the two notions.

Example 9.7. The forms $ax^2 + bxy + cy^2$ and $ax^2 - bxy + cy^2$ are always (improperly) equivalent via $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. However sometimes they are properly equivalent (e.g. $2x^2 \pm 2xy + 3y^2$) and sometimes they are not (e.g. $3x^2 \pm 2xy + 5y^2$).

Lemma 9.8. *A bqf $f(x, y)$ properly represents an integer m if and only if $f(x, y)$ is properly equivalent to $mx^2 + bxy + cy^2$ for some $b, c \in \mathbb{Z}$.*

Proof. Assume m is properly represented by $f(x, y)$. The there exist relatively prime integers α, γ such that $f(\alpha, \gamma) = m$. Since $(\alpha, \gamma) = 1$, there exist integers β, δ such that

$$\alpha\delta - \beta\gamma = 1 \iff \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

Then

$$f(\alpha x + \beta y, \gamma x + \delta y) = f(\alpha, \gamma)x^2 + [f(\alpha, \delta) + f(\beta, \gamma)]\, xy + f(\beta, \delta)y^2,$$

which is of the desired form since $f(\alpha, \gamma) = m$.
Conversely, note that $g(x, y) = mx^2 + bxy + cy^2$ properly represents m because $m = g(1, 0)$. □

Proposition 9.9. *(i) Two equivalent bqf's represent the same integers.*

(ii) Two equivalent bqf's properly represent the same integers.

(iii) If a bqf $f(x, y)$ is equivalent to a primitive bqf, then $f(x, y)$ itself is primitive.

Proof. Exercise. □

Definition. *The discriminant of the bqf $ax^2 + bxy + cy^2$ is the integer $D = b^2 - 4ac$.*

Proposition 9.10. *Two equivalent forms have the same discriminant.*

Proof. Exercise. □

The discriminant D has a strong effect on the behavior of the bqf $f(x, y) = ax^2+bxy+cy^2$. We have

$$4af(x, y) = (2ax + by)^2 - Dy^2. \tag{9.1}$$

Thus, if $D < 0$, then $4af(x, y) \geq 0$, so the form represents either only nonnegative integers if $a > 0$ or only nonpositive integers if $a < 0$. (Note that we cannot have $a = 0$, since that would make $D = b^2$ which cannot be negative.)

On the other hand, if $D > 0$ then

$$f(b, -2a) = -aD$$

and

$$f(1, 0) = a$$

have opposite signs whenever $a \neq 0$. When $a = 0$, $D = b^2 > 0$ so $b \neq 0$ and $f(x, y) = bxy + cy^2 = y(bx + cy)$. Then $f(-c+1, b) = b(-bc+b+bc) = b^2 = D > 0$ and $f(-c-1, b) = -b^2 = -D < 0$. Therefore $f(x, y)$ represents both positive and negative integers.

Definition. *A bqf $f(x, y) = ax^2 + bxy + cy^2$ is called*

- *positive definite if $D < 0, a > 0$. It cannot represent negative integers.*
- *negative definite if $D < 0, a < 0$. It cannot represent positive integers.*
- *indefinite if $D > 0$. It represents both positive and negative integers ($D > 0$).*

Note: The above notions are invariant under equivalence.

Examples:

- $x^2 + ny^2$ is positive definite when $n > 0$.
- $x^2 + 3xy + y^2$ is indefinite
- $-x^2 + 3xy - 13y^2$ is negative definite.

The discriminant D influences the form in one other way. Since $D = b^2 - 4ac$ it follows that

$$D \equiv b^2 \pmod 4 \equiv 0, 1 \pmod 4.$$

Proposition 9.11. *Let $D \equiv 0, 1 \pmod 4$ be an integer and m be an odd integer such that $(m, D) = 1$. Then m is properly represented by a primitive bqf of discriminant D if and only if D is a quadratic residue modulo m.*

Proof. First assume m is properly represented by a primitive form $g(x, y)$. By Lemma 9.8, $g(x, y)$ is properly equivalent to a form $f(x, y) = mx^2 + bxy + cy^2$ where $b, c \in \mathbb{Z}$. By Proposition 9.9, $f(x, y)$ is also primitive and by Proposition 9.10, m is properly represented by $f(x, y)$. The discriminant of $f(x, y)$ is $D = b^2 - 4mc \equiv b^2 \pmod m$, so D is a quadratic residue modulo m.
Conversely, suppose $D \equiv b^2 \pmod m$. Since m is odd, we assume that D and b have the same parity (replace b by $b+m$ if necessary). Since $D \equiv 0, 1 \pmod 4$ it follows that $4 \mid D - b^2$ and thus

$$D \equiv b^2 \pmod{4m}.$$

Hence there exists $c \in \mathbb{Z}$ such that $D = b^2 - 4mc$.
Therefore $f(x, y) = m^2 + bxy + cy^2$ properly represents m (by Lemma 9.8) and has discriminant D. Since $(m, D) = 1$ it follows that $f(x, y)$ is primitive. □

Corollary 9.12. *Let $n \in \mathbb{Z}$ and p be an odd prime that does not divide n. Then $\left(\dfrac{-n}{p}\right) = 1$ if and only if p is represented by a primitive form of discriminant $-4n$.*

Proof. This follows immediately from Proposition 9.11, since p is prime and therefore $-4n$ is a quadratic residue modulo p if and only if $1 = \left(\dfrac{-4n}{p}\right) = \left(\dfrac{-n}{p}\right)$. □

This corollary gives an inkling into how to represent the primes that divide numbers of the form $a^2 + nb^2, (a, b) = 1$. Namely, we have seen that these primes are the ones for which $\left(\frac{-n}{p}\right) = 1$. Corollary 9.12 tells us that such primes are represented by some bqf of discriminant $-4n$.

The problem is that there are too many bqf of discriminant $-4n$. For instance, all the forms that appear in Euler's Conjecture 9.2 have discriminant -56. Or, apply the proof of Proposition 9.11 to $n = 3$ (so $D = -12$) and $m = 13$. Since $\left(\frac{-3}{13}\right) = 1$, Proposition 9.11 implies that 13 is represented by some bqf of discriminant -12. Going through the proof, we have to find b even such that

$$D \equiv b^2 \pmod{4m} \iff -12 \equiv b^2 \pmod{52}.$$

Going through $-12 \pmod{52} = \{\ldots, -12, 40, 92, 144 = 12^2, \ldots\}$ we see that we can take $b = 12$. Next, we need to find c such that

$$D = b^2 - 4mc \iff -12 = 144 - 52c \iff c = 3.$$

Thus 13 is represented by the bqf $f(x,y) = 13x^2+12xy+3y^2$ (which has indeed discriminant -12). This is not exactly enlightening. What we need is a way to produce simpler bqf's that represent a given integer.

From now on we restrict our attention to primitive, positive definite binary quadratic forms. Happily enough, the forms $x^2 + ny^2 (n > 0)$ that we care about are indeed primitive and positive definite.

Definition. *A primitive positive definite bqf* $ax^2 + bxy + cy^2$ *is* reduced *if*

$$0 \leq |b| \leq a \leq c \quad \text{and} \quad b \geq 0 \text{ if either } |b| = a \text{ or } a = c. \tag{9.2}$$

Note: The integers a, c must be positive since the form is positive definite.

Examples:

- If $n > 0$, then $x^2 + ny^2$ is reduced.
- $2x^2 + 7y^2$ is reduced.
- $13x^2 + 12xy + 3y^2$ is primitive and positive definite, but not reduced.

Theorem 9.13. *Any primitive positive definite bqf is properly equivalent to a* unique *reduced form.*

Proof. Our proof has three steps.
Step 1 We show that a given primitive, positive definite bqf $f(x,y)$ is equivalent to a primitive positive definite bqf $f(x,y) = ax^2 + bxy + cy^2$ with $0 \leq |b| \leq a \leq c$.

Among all the forms properly equivalent to $g(x,y)$ – which we already know that have to be primitive and positive definite – choose the one with the minimal coefficient of xy. That is, choose $f'(x,y) = a'x^2 + b'xy + c'y^2$ such that $|b'|$ is minimal. Assume by contradiction that $a' < |b'|$. Then, for any integer m,

$$g'(x,y) = g'(x + my, y) = a'x^2 + (2a'm + b')xy + (c' + a'm^2)y^2$$

is properly equivalent to our $g(x,y)$. Since $a' < |b'|$ we can choose $m \in \mathbb{Z}$ (think quotient of division of $|b'|$ by $2a$) such that $0 \leq |2a'm + b'| < |b'|$. This contradicts the minimality of $|b'|$, so $|b'| \leq a'$. Similarly, we get $|b| \leq c'$. If $a' \leq c'$, choose $f(x,y) = f'(x,y)$ (and $b = b'$, $|b| \leq a = a' \leq c' = c$). If $a' > c'$, take $f(x,y) = f'(-y,x) = a'y^2 - bxy + c'x^2$ and $b = -b'$, $|b| = |b'| < a = c' < a' = c$. (i.e. interchange a' and c' and change the sign of b'). Note that $(x,y) \mapsto (-y,x)$ induces a proper equivalence since

$$\det \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = 1.$$

Step 2 We show that a primitive positive definite bqf $f(x,y) = ax^2 + bxy + cy^2$ with $0 \leq |b| \leq a \leq c$ is properly equivalent to a reduced one.

The form $f(x,y)$ is already reduced unless $b < 0$ and $-b = a$ or $a = c$. But then $f'(x,y) = ax^2 - bxy + cy^2$ is reduced and all we have to show is that $f(x,y)$ and $f'(x,y)$ are properly equivalent.

If $a = -b$: $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ and

$$f(A\vec{x}) = f(x+y, y) = a(x+y)^2 - a(x+y)y + cy^2 = ax^2 + axy + cy^2 = f'(x,y).$$

If $a = c$: $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ and

$$f(B\vec{x}) = f(-y, x) = ay^2 - bxy + ax^2 = f'(x,y).$$

Step 3 We show that two reduced forms cannot be properly equivalent.
Let $f(x,y) = ax^2 + bxy + cy^2$ with $|b| \le a \le c$. Since $f(x,y)$ is positive definite, for any integers x, y we have

$$f(x,y) \ge (a - |b| + c)\min(x^2, y^2) \text{ (exercise!)}$$

Therefore

$$f(x,y) > a - |b| + c \ge a \text{ whenever } xy \ne 0. \tag{9.3}$$

On the other hand $f(x,0) = ax^2$ and $f(0,y) = cy^2$. As we have seen in Example 9.3, a is properly represented by $f(x,y)$ and (9.3) implies that a is the smallest nonzero value of $f(x,y)$. Moreover, if $c > a$ then c is the next smallest positive value of $f(x,y)$. (Because f *Therefore the coefficients of x^2 and y^2 of a reduced form are the smallest positive integers properly represented by any equivalent form.* (This observation is due to Legendre.) For simplicity, assume $f(x,y) = ax^2 + bxy + cy^2$ is a reduced from with $|b| < a < c$. (The other cases are left as exercise.) From what we discussed above, it follows that $a < c < a - |b| + c$ are the smallest numbers properly represented by $f(x,y)$.

$$\begin{aligned} \textbf{Claim} \quad & f(x,y) = a,\ (x,y) = 1 \iff x = \pm 1, y = 0 \\ & f(x,y) = c,\ (x,y) = 1 \iff x = 0, y = \pm 1. \end{aligned} \tag{9.4}$$

Assume that $g(x,y) = a'x^2 + b'xy + c'y^2$ is a reduced form equivalent to $f(x,y)$. Since $f(x,y)$ and $g(x,y)$ represent the same numbers and are reduced, they must have the same coefficient of x^2 by Legendre's observation. So $a = a'$. On the other hand, $c' \ge a$. Assume that $c' = a$. Then, by (9.4), the equation $g(x,y) = a$ has 4 proper solutions $\pm(1,0), \pm(0,1)$. But the equation $f(x,y) = a$ has only 2 proper solutions (contradiction). Hence $c' > a$ and by applying again Legendre's observation, it follows that $c = c'$. Since the two bqf's have the same discriminant, it follows that $|b'| = |b|$. Thus

$$g(x,y) = ax^2 \pm bxy + cy^2.$$

It remains to show that $f(x,y) = g(x,y)$ when we make the stronger assumption that the two bqf's are *properly equivalent.* That is, we now assume that we have

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \quad g(x,y) = f(\alpha x + \beta y, \gamma x + \delta y).$$

Then

$$a = g(1,0) = f(\alpha,\gamma) \quad c = g(0,1) = f(\beta,\delta).$$

Since $\det A = 1$, we have $\alpha\delta - \beta\gamma = 1$, so $(\alpha,\gamma) = 1$ and $(\beta,\delta) = 1$. By (9.4), it follows that $(\alpha,\gamma) = \pm(1,0)$ and $(\beta,\delta) = \pm(0,1)$. Since $\det A = 1$, it follows that

$$A = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

and therefore $f(x,y) = g(x,y)$.

□

Note: Now we can justify the examples we gave of properly equivalent and improperly equivalent forms. Namely, $3x^2 \pm 2xy + 5y^2$ (which we know are equivalent) are both reduced, and therefore they cannot be properly equivalent. Thus they are improperly equivalent. On the other hand, $2x^2 \pm 2xy + 3y^2$ are equivalent, but only $2x^2 + 2xy + 3y^2$ is reduced. By the proof of Theorem 9.13, the two forms properly equivalent.

From now on, all bqf's will be primitive, positive definite and equivalence will be proper.

Definition. *The class number of $h(D)$ is the number of classes of primitive positive definite forms of discriminant $D < 0$.*

Note: By Theorem 9.13, $h(D)$ is equal to the number of reduced forms of discriminant D. A priori this number has no reason to be finite. However, suppose $ax^2 + bxy + cy^2$ to be a reduced form of discriminant $D < 0$. Since $|b| \leq a$ we have $b^2 \leq a^2$. Combining this with $a \leq c$, we get

$$-D = 4ac - b^2 \geq 4a^2 - b^2 \geq 4a^2 - a^2 = 3a^2 \implies 0 \leq a \leq \sqrt{\frac{-D}{3}}.$$

If D is fixed, then the above relation and the fact $|b| \leq a$ imply that there are only finitely many choices for a and b. Moreover, each such choice fixes c since $D = b^2 - 4ac$.
Thus there are only finitely many reduced forms of discriminant D and we have proved the following result.

Theorem 9.14. *Let $D \in \mathbb{Z}_{<0}$. The class number $h(D)$ is finite and is equal to the number of reduced forms of discriminant D.*

Here are a couple of examples computed using the algorithm described above. We will need to use some of them later on, and I might explain them in class. But it would be a good idea to work as many of them as you can on your own.

D	$h(D)$	reduced forms of discriminant D
-4	1	x^2+y^2
-8	1	x^2+2y^2
-12	1	x^2+3y^2
-20	2	$x^2+5y^2, 2x^2+2xy+3y^2$
-28	1	x^2+7y^2
-56	4	$x^2+14y^2, 2x^2+7y^2, 3x^2\pm 2xy+5y^2$
-108	3	$x^2+27y^2, 4x^2\pm 2xy+7y^2$
-256	4	$x^2+64y^2, 4x^2+4xy+17y^2, 5x^2\pm 2xy+13y^2$

We can now go back to the Descent Step in Euler's strategy.

Theorem 9.15. *Let $n \in \mathbb{Z}_{>0}$ and p be an odd prime such that $p \nmid n$. Then $\left(\frac{-n}{p}\right) = 1$ if and only if p is represented by one of the $h(-4n)$ reduced forms of discriminant $-4n$.*

Proof. This is an immediate consequence of Corollary 9.12 and Theorem 9.13. □

This result completely settles the Descent Step. We just need to put it together with the Reciprocity Step, and see what we get. But rather than looking at the case of bqf's of discriminant $-4n$, we will state a result that applies to all discriminants $D < 0$.

Theorem 9.16. *Let D be a negative integer such that $D \equiv 0, 1 \pmod 4$. Let $\chi = \chi_D : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ be the group homomorphism defined in Theorem 8.17 and p be an odd prime, $p \nmid D$. Then $p \pmod D \in \ker \chi$ if and only if p is represented by one of the $h(D)$ reduced forms of discriminant D.*

Proof. We have seen that

$$p \pmod D \in \ker \chi \iff \left(\frac{D}{p}\right) = 1.$$

We also know that

$$\left(\frac{D}{p}\right) = 1 \iff D \text{ is a quadratic residue modulo } p.$$

By Proposition 9.11 this is equivalent to the fact that p is represented by a primitive positive definite form of discriminant D. The result now follows from Theorem 9.13. □

This theorem tells us that there is a congruence condition $p \equiv \alpha, \beta, \ldots \pmod D$ which gives necessary and sufficient conditions for an odd prime $p \nmid D$ to be represented by a form of discriminant D. Since we know how to find the reduced forms of a given discriminant and quadratic reciprocity makes it easy to find the congruence classes $\alpha, \beta, \ldots \pmod D$ such that $\left(\frac{D}{p}\right) = 1$, we now have a complete and effective form of Euler's strategy.

Example 9.17. $D = -4$: the only reduced form is $x^2 + y^2$. On the other hand we know that

$$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4.$$

Thus it follows immediately from Theorem 9.16 that $p \neq 2$ is of the form $x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$.

In other words, now we get a two line proof of a fact that had taken all of Section 2 to prove before.

$D = -8$: again we have only one reduced form of discriminant -8, namely $x^2 + 2y^2$. And we know that

$$\left(\frac{2}{p}\right) = 1 \iff p \equiv 1, 3 \pmod 8.$$

Theorem 9.16 implies that $p \neq 2$ is of the form $x^2 + 2y^2$ if and only if $p \equiv 1, 3 \pmod 8$. I won't remind you how long that took to prove!

$D = -12$: the only reduced form is $x^2 + 3y^2$ and it is easy to see find the congruence classes for p so that $\left(\frac{-3}{p}\right) = 1$.

We can go further than Fermat.

Proposition 9.18. *If p is a prime, then*

$$p = x^2 + 7y^2 \iff p = 7 \text{ or } p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}.$$

Proof. Exercise. □

Each time we made use of the fact that there is only one reduced form of discriminant $-4n$, i.e. that $h(-4n) = 1$. Unfortunately, the list of $n > 0$ for which this happens is rather short.

Theorem 9.19 (Landau)**.** *Let n be a positive integer. Then*

$$h(-4n) = 1 \iff n = 1, 2, 3, 4, 7.$$

Proof. We will follow Landau. In a nutshell, the idea is that we already know a reduced from of discriminant $-4n$, namely $x^2 + ny^2$. So if we produce another one, that means that $h(-4n) > 1$. We already know that $h(-4) = 1$, so we can assume that $n > 1$. If n is *not* a prime power, it means that n has at least two distinct prime divisors p and q. Therefore

$$n = p^r q^s m, \text{ with } r, s \geq 1 \text{ and } (m, p) = (m, q) = 1.$$

Choose $a = \min(p^r, q^s)$ and $c = m \cdot \max(p^r, q^s)$.Then $n = ac$, $c > a > 1$ and $(a, c) = 1$. Therefore the form

$$ax^2 + cy^2$$

is reduced of discriminant $-4n$.

If $n = 2^r$ and $r \geq 4$, then

$$4x^2 + 4xy + (2^{r-2} + 1)y^2$$

is reduced (note that $4 \leq 2^{r-2} + 1$ since $r \geq 4$) of discriminant $-4n$.

If $n = 2^3$, then we follow the algorithm for finding reduced forms of discriminant $D = -4 \cdot 8 = -32$. We know that

$$0 < a \leq \sqrt{\frac{32}{3}} \implies 1 \leq a \leq 3.$$

If $a = 3$, then $|b| \leq 3$. But if $b = \pm 3$, this means that we have to find $c \in \mathbb{Z}$ such that $-32 = 9 - 12c$ which is impossible. For $b = \pm 2$ we get $-32 = 4 - 12c$, so $c = 3$. But then only $3x^2 + 2xy + 3y^2$ is reduced. However this is enough for our purposes, because it shows that $h(-32) > 1$. (In fact, $h(-32) = 2$, which is left as an exercise.)

Of the powers of 2 this leaves us with $n = 2, 4$. We have already seen what happens for $n = 2$. The case $n = 4$ is left as an exercise.

If $n = p^r$ with p and odd prime, then $n + 1$ is even. So if $n + 1$ is a *not* a power of 2, then $n + 1 = ac$ with $1 < a < c$ and $(a, c) = 1$. It follows that

$$ax^2 + 2xy + cy^2$$

is reduced of discriminant $-4n$. If $n + 1 = 2^s$ and $s \geq 6$, then

$$8x^2 + 6xy + (2^{s-3} + 1)y^2$$

is reduced (indeed, $8 < 2^{s-3} + 1$ in this case) of discriminant $-4n$.
If $s = 5$, then $n + 1 = 32$, so $n = 31$ which is an odd prime. We go through our algorithm again to find reduced forms with discriminant $-4n = -124$. We have

$$0 < a \leq \sqrt{\frac{124}{3}} \implies 1 \leq a \leq 5.$$

Now we need to find an integer solution to the equation $-124 = b^2 - 4ac$ with $|b| \leq a \leq c$. First note the b has to be even. If $a = 5$ and $b = \pm 4$ the equation becomes $-124 = 16 - 20c$, so $c = 7$. The forms

$$5x^2 \pm 4xy + 7y^2$$

are both reduced of the given discriminant, so $h(-4n) \geq 3$. (In fact we have equality, a fact that I leave for you to prove!).
For $s = 4$ we get $n + 1 = 16 \implies n = 15$ which is not a prime power.
For $s = 3$ we get $n+1 = 8 \implies n = 7$ and we have seen in Proposition 9.18 that $h(-28) = 1$.
For $s = 2$ we get $n + 1 = 4 \implies n = 3$ and we have seen in Example 9.17 that $h(-12) = 1$.
For $s = 1$ we get back to $n = 1$. □

Note: The case $n = 4$ is included in the $p = x^2 + y^2$ case since one of the x, y has to be even and the other odd in order for p to be odd.

9.1 Elementary genus theory

Landau's Theorem 9.19 makes it clear that we need some new ideas for dealing with the case $h(-4n) > 1$. Let us consider the following example.

Example 9.20. Take the case $n = 5$. First let us determine the reduced form of discriminant $D = -20$. We have seen that they need to satisfy

$$0 \leq |b| \leq a \leq \sqrt{\frac{20}{3}} \implies 0 \leq |b| \leq a \leq 2,$$

and $-20 = b^2 - 4ac$ so b is even.

- $a = 2$: then $-20 = b^2 - 8c$.
  If $b = 2$, then $c = 3$ and we get the reduced form $2x^2 + 2xy + 3y^2$.
  If $b = 0$, the diophantine equation has no solution $c \in \mathbb{Z}$.
- $a = 1$: then $b = 0$ and $20 = -4c$, so $c = 5$. This yields the familiar $x^2 + 5y^2$.

Therefore $h(-20) = 2$ and the two reduced form are

$$2x^2 + 2xy + 3y^2 \quad \text{and} \quad x^2 + 5y^2.$$

Here Theorem 9.16 and quadratic reciprocity tell us that, if $p \neq 5$ is an odd prime

$$p \equiv 1, 3, 7, 9 \pmod{20} \iff \left(\frac{-5}{p}\right) = 1 \iff p = x^2 + 5y^2 \text{ or } p = 2x^2 + 2xy + 3y^2.$$

We can see from this example that what we need is a method to separate reduced forms of the same discriminant. The basic idea is due to Lagrange: consider the congruence classes in $(\mathbb{Z}/D\mathbb{Z})^\times$ represented by a single form and group together the forms that represent the same congruence classes. This is precisely the basic idea of genus theory.

To clarify what we mean, we look again at the case $D = -20$. We will plug in for x, y all the values in $\mathbb{Z}/D\mathbb{Z}$ and for each pair compute the value of the two reduced forms of genus D. Then we throw out the pairs that give values that are not in $(\mathbb{Z}/D\mathbb{Z})^\times$. To shorten our computation, note that if both x, y are divisible by 2 or 5, then so will both $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$. So at least one of them has to be relatively prime to 20.

$x \pmod{20}$	$y \pmod{20}$	x^2+5y^2		$2x^2+2xy+3y^2$	
0	± 1	5	(throw this out)	3	(keep this one)
0	± 3	5	(throw this out)	7	(keep this one)
0	± 7	5	(throw this out)	7	(keep this one)
0	± 9	5	(throw this out)	3	(keep this one)
± 1	0	1	(keep this one)	2	(throw this out)
± 3	0	9	(keep this one)	18	(throw this out)
± 7	0	9	(keep this one)	18	(throw this out)
± 9	0	1	(keep this one)	2	(throw this out)
1	1	6	(throw this out)	7	(keep this one)
1	2	1	(keep this one)	18	(throw this out)
$\vdots$	$\vdots$	$\vdots$		$\vdots$	

Continuing this table one sees that

$$\begin{aligned} x^2+5y^2 \text{ represents} &\qquad 1,9 \text{ in } (\mathbb{Z}/20\mathbb{Z})^\times \\ 2x^2+2xy+3y^2 \text{ represents} &\qquad 3,7 \text{ in } (\mathbb{Z}/20\mathbb{Z})^\times \end{aligned} \tag{9.5}$$

Repeating the same procedure for $D=-56$, we get that

$$\begin{aligned} x^2+14y^2,\ 2x^2+7y^2 \text{ represent} &\qquad 1,9,15,23,25,39 \text{ in } (\mathbb{Z}/56\mathbb{Z})^\times \\ 3x^2 \pm 2xy+5y^2 \text{ represent} &\qquad 3,5,13,19,27,45 \text{ in } (\mathbb{Z}/56\mathbb{Z})^\times \end{aligned} \tag{9.6}$$

Definition. *We say that two primitive positive definite bqf's of discriminant D have the same* genus *if they represent the same congruence classes in* $(\mathbb{Z}/D\mathbb{Z})^\times$.

Note: Since equivalent forms represent the same integers, they are in the same genus. In particular, each genus consists of a finite number of proper classes of forms.

In (9.5), we have seen that for $D=-20$ there are 2 genera, each consisting of a single class. Combining the same (9.5) with Theorem 9.16 we obtain that for an odd prime $p \neq 5$,

$$\begin{aligned} p = x^2+5y^2 &\iff p \equiv 1,9 \pmod{20} \\ p = 2x^2+2xy+3y^2 &\iff p \equiv 3,7 \pmod{20} \end{aligned} \tag{9.7}$$

So we now have a proof for the first part of Euler's Conjecture 9.1.

On the other hand, (9.6) shows that for $D=-56$ there are also 2 genera, but now each genus consists of 2 classes. Combining it with Theorem 9.16 we obtain that for an odd prime $p \neq 7$,

$$\begin{aligned} p = x^2+14y^2 \text{ or } p = 2x^2+7y^2 &\iff p \equiv 1,9,15,23,25,39 \pmod{56} \\ p = 3x^2 \pm 2xy+5y^2 &\iff p \equiv 3,5,13,19,27,45 \pmod{56} \end{aligned} \tag{9.8}$$

This proves first part of Euler's Conjecture 9.2.

In both these cases, what made the whole thing work was the fact the the two genera represent disjoint sets of values in $(\mathbb{Z}/D\mathbb{Z})^\times$. We must show that this phenomenon holds in general. To that end, we start with a result of Gauss.

Lemma 9.21. *Given a form $f(x,y)$ and an integer $M \neq 0$, the bqf $f(x,y)$ properly represents numbers relatively primes to M.*

Proof. Let $f(x,y) = ax^2 + bxy + cy^2$. We know that $(a,b,c) = 1$ – since all our forms are primitive – so no prime can divide all of them. Let p be an arbitrary prime. There are three possibilities.

- $p \mid a$ and $p \mid c$: then $p \nmid b$. Therefore if $p \nmid x$ and $p \nmid y$, then $p \nmid f(x,y)$.
- $p \nmid a$: choose x, y such that $p \nmid x$ and $p \mid y$. Then $p \nmid f(x,y)$.
- $p \nmid c$: choose x, y such that $p \mid x$ and $p \nmid y$. Then $p \nmid f(x,y)$.

If $M = \pm 1$, the result is obvious. If not, then $M = \pm p_1^{a_1} \dots p_r^{a_r}$ with $p_1, \dots, p_r$ distinct primes. By the Chinese Remainder Theorem we can choose x, y subject to the above conditions for each of the $p_i, 1 \leq i \leq r$. Then $p_i \nmid f(x,y)$ for all i and therefore $m = f(x,y)$ is relatively prime to M. The result follows since, by Lemma 9.4, $m = d^2 m'$ for some m' that is properly represented by $f(x,y)$. □

Definition. *For a negative integer $D \equiv 0, 1 \pmod 4$ the* principal form *of discriminant D is*

$$x^2 - \frac{D}{4}y^2 \qquad \text{if } D \equiv 0 \pmod 4$$

$$x^2 + xy + \frac{1-D}{4}y^2 \qquad \text{if } D \equiv 1 \pmod 4.$$

Note: These forms have indeed discriminant D and they are reduced.

Proposition 9.22. *Given a negative integer $D \equiv 0, 1 \pmod 4$, denote by $\chi = \chi_D : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ the group homomorphism defined in Theorem 8.17. Let $f(x,y)$ be a bqf of discriminant D.*

(i) The values in $(\mathbb{Z}/D\mathbb{Z})^\times$ represented by the principal form of discriminant D form a subgroup $H \subset \ker\chi \subset (\mathbb{Z}/D\mathbb{Z})^\times$.

(ii) The values in $(\mathbb{Z}/D\mathbb{Z})^\times$ represented by $f(x,y)$ form a coset of H in $\ker\chi$.

Note: Since cosets are disjoint, this says that different genera represent disjoint sets of values in $(\mathbb{Z}/D\mathbb{Z})^\times$. It also means that each genus corresponds to an element of the quotient group $(\ker\chi)/H$.

Proof. We start by proving that if a number $(m, D) = 1$ is represented by a form $g(x, y)$ of discriminant D, then $[m] \in \ker \chi$. By Lemma 9.4, $m = d^2 m'$ where m' is properly represented by $g(x, y)$. Then

$$\chi([m]) = \chi([d^2 m']) = \chi([d])^2 \chi([m']) = \chi([m']).$$

On the other hand, Proposition 9.11 implies that D is a quadratic residue modulo m', so there exist integers $b, c \in \mathbb{Z}$ such that $D = b^2 - cm'$. Note that $(b, m') = 1$. If m' is odd, then

$$\chi([m]) = \chi([m']) = \left(\frac{D}{m'}\right) = \left(\frac{b^2 - cm'}{m'}\right) = \left(\frac{b^2}{m'}\right) = \left(\frac{b}{m'}\right)^2 = 1.$$

If m' is even, then D must be odd and Lemma 9.8 implies that m' is (properly) represented by a form $m'x^2 + b'xy + c'y^2$ of discriminant D. Hence

$$D = (b')^2 - 4m'c' \equiv (b')^2 \pmod 8.$$

But b' has to be odd, and the only odd square modulo 8 is 1. Hence $D \equiv 1 \pmod 8$, and by a homework exercise, this implies that $\chi([2]) = 1$. Therefore, if we write $m' = 2^a m''$ we have

$$\chi([m]) = \chi([m']) = \chi([2])^a \chi([m'']) = \chi([m'']) = 1 \text{ (as before)}.$$

Now that our claim is proved, let us go back to the first statement of the Proposition. By definition

$$H = \{[m];\ m \text{ is represented by the principal form of discriminant } D\}.$$

The above claim shows that the set H is a subset of $\ker \chi$. We have to show that H contains the identity (and this is trivial since the principal form evaluated at $(1, 0)$ yields precisely 1) and is closed under multiplication.

- When $D = -4n$, the principal form is $x^2 + ny^2$. But we know that

  $$(x^2 + ny^2)(u^2 + nv^2) = (xu + nyv)^2 + n(xv - yu)^2.$$

  Therefore the product of two representable integers is also representable.

- When $D = 1 - 4n$, the principal form is $x^2 + xy + ny^2$. We have

  $$4(x^2 + xy + ny^2) \equiv 4x^2 + 4xy + y^2 \pmod D \equiv (2x + y)^2 \pmod D. \tag{9.9}$$

  Let $H' = \{[m]^2; [m] \in (\mathbb{Z}/D\mathbb{Z})^\times\}$ the subgroup of squares in $(\mathbb{Z}/D\mathbb{Z})^\times$. Then (9.9) shows that $H = H'$ and therefore H is closed under multiplication.

For the second statement of the Proposition, we again treat the two cases separately. If $D = -4n$, then taking $M = 4n$ in Lemma 9.21 we obtain that $f(x, y)$ properly represents some integer a relatively prime to D. By Lemma 9.8, we get that $f(x, y)$ is properly equivalent to a bqf of the form $ax^2 + b'xy + cy^2$ of discriminant D. Since representability is stable under

equivalence of forms, we can assume that $f(x,y) = ax^2 + b'xy + cy^2$.
But $-4n = D = (b')^2 - 4ac$, so b' is even. Therefore

$$f(x,y) = ax^2 + 2bxy + cy^2 \text{ and } n = ac - b^2.$$

Therefore

$$af(x,y) = (ax + by)^2 + ny^2.$$

Since $(a, 4n) = 1$ it follows that the values of $f(x,y)$ in $(\mathbb{Z}/4n\mathbb{Z})^\times$ lie in the coset $[a]^{-1}H$.
Conversely, if $[m] \in [a]^{-1}H$, then $[ac] \in H$, so there exist integers u, v such that

$$am \equiv u^2 + nv^2 \pmod{4n}.$$

Choose $x, y \in \mathbb{Z}$ such that

$$\begin{cases} ax + by & \equiv u \pmod{4n} \\ y & \equiv v \pmod{4n}. \end{cases}$$

Note that we can do this since $(a, 4n) = 1$. Then

$$af(x,y) = (ax + by)^2 + ny^2 \equiv u^2 + nv^2 \pmod{D} \equiv am \pmod{D}.$$

Again we use the fact that $(a, D) = 1$ to obtain

$$f(x,y) \equiv m \pmod{D} \implies [m] \text{ is represented by } f(x,y).$$

The case $D \equiv 1 \pmod 4$ is similar (exercise!) and the result is proved. □

Definition. *With the notation from Proposition 9.22, let H' be a coset of H in* $\ker \chi$. *The* genus *of the coset H' consists of all the forms of discriminant D that represent the values of H' modulo D.*
The genus containing the principal form is called the principal genus.

We have proved the following result.

Theorem 9.23. *Let $D < 0$ be an integer such that $D \equiv 0, 1 \pmod 4$ and $p \nmid D$ be an odd prime. With the notation from Proposition 9.22, let H' be a coset of H in* $\ker \chi$. *Then $[p] = p \pmod D \in H'$ if and only if p is represented by a reduced form of discriminant D in the genus of H'.*

This is the main result of our elementary genus theory. It generalizes (9.7) and (9.8), and it shows that there are always congruence conditions which characterize the primes that can be represented by some bqf in a given genus.

For us, the most interesting situation regards the principal genus, since for $D = -4n$ the principal form is $x^2 + ny^2$.

Corollary 9.24. *Let $n \in \mathbb{Z}> 0$ and $p \nmid n$ and odd prime. Then p is represented by a form of discriminant $-4n$ in the principal genus if and only if there exist an integer β such that*

$$p \equiv \beta^2 \text{ or } \beta^2 + n \pmod{4n}.$$

Proof. If y is even, then $x^2 + ny^2 \equiv x^2 \pmod{4n}$.
On the other hand, if y is odd, then $x^2 + ny^2 \equiv x^2 + n \pmod{4n}$.

□