Chapter 8
Counting Pythagorean triples modulo an integer

In this chapter we study the Pythagorean Equation in integers modulo a natural number n and count the number of solutions. In the first section we consider the case where n is a prime number. Later in the chapter we discuss the general case. By using the Chinese Remainder Theorem we show that in order to count the number of solutions modulo a natural number n, it suffices to count the number of solutions modulo prime power divisors of n. We then devise a recursive process to count the number of solutions modulo prime powers. At the end of the chapter we show how the recursive process introduced earlier can be used to find solutions of equations such as $x^2 \equiv 2 \bmod 7^k$ for any natural number k. We will, for example, show that for each k, this equation has precisely two solutions modulo 7^k. The strategy used here is what is usually called Hensel's Lemma. We explore this lemma in Exercises 8.4 and 8.5. In the Notes, we discuss p-adic numbers. We finish with the statement of Hilbert's Law of Reciprocity which is a massive generalization of the Gauss's Law of Quadratic Reciprocity.

8.1 The Pythagorean Equation modulo a prime number p

One interesting feature of the geometric method discussed in §3.2 and explored further in §3.3 is that one does not need to do the geometric constructions presented there just in the real plane. One can repeat the same constructions over every field, provided that one cares that the denominators of the fractions that appear are not zero. This is not an issue over the real numbers, and obviously over the rationals, as for m a real number, $m^2 + 1$ is never zero. But as soon as we start working over the complex numbers, there are in fact choices for m that make $m^2 + 1$ equal to zero. The same problem occurs when considering the Pythagorean Equation modulo a prime number p.

We start by determining $N_p := \#S_p$ with

R. Takloo-Bighash, *A Pythagorean Introduction to Number Theory*,
Undergraduate Texts in Mathematics, https://doi.org/10.1007/978-3-030-02604-2_8

$$S_p = \{(x, y) \mid 1 \le x, y \le p,\ x^2 + y^2 \equiv 1 \bmod p\}.$$

Let's examine a few small primes. We have

$$S_3 = \{(0, 1), (0, 2), (1, 0), (2, 0)\}, \quad N_3 = 4 = 3 + 1;$$

$$S_5 = \{(0, 1), (0, 4), (1, 0), (4, 0)\}, \quad N_5 = 4 = 5 - 1;$$

$$S_7 = \{(0, 1), (0, 6), (1, 0), (6, 0), (2, 2), (2, 5), (5, 2), (5, 5)\}, \quad N_7 = 8 = 7 + 1;$$

$$S_{11} = \{(0, 1), (0, 10), (1, 0), (10, 0), (3, 6), (3, 5), (8, 6), (8, 5),$$
$$(6, 3), (5, 3), (6, 8), (5, 8)\}, \quad N_{11} = 12 = 11 + 1;$$

$$S_{13} = \{(0, 1), (0, 12), (1, 0), (12, 0), (2, 6), (2, 11), (11, 6), (11, 7),$$
$$(6, 2), (11, 2), (6, 11), (7, 11)\}, \quad N_{13} = 12 = 13 - 1.$$

In these examples, $N_p = p - a(p)$ with $a(p) = +1$ whenever p is of the form $4k + 1$, for $p = 5, 13$, and $a(p) = -1$ when p is of the form $4k + 3$, for $p = 3, 7, 11$. Equation 6.3 shows that at least for these primes $a(p) = (-1/p)$. So a reasonable guess is

$$N_p = p - \left(\frac{-1}{p}\right).$$

We will show that this is indeed the case. In order to prove our guess we first find a parametrization for all the solutions of the equation $x^2 + y^2 \equiv 1 \bmod p$. There are several obvious solutions, e.g., $(-1, 0)$ as in the real case. Fix a residue class $m \bmod p$. We consider the intersection of the "line" of "slope" m passing through $(-1, 0)$, i.e., the collection of pairs (x, y) with $1 \le x, y \le p$ such that

$$y \equiv m(x + 1) \mod p,$$

with the "circle" $x^2 + y^2 \equiv 1 \bmod p$. As before, we obtain

$$m^2(x + 1)^2 + x^2 \equiv 1 \mod p,$$

or

$$(m^2 + 1)x^2 + 2m^2x + (m^2 - 1) \equiv 0 \mod p.$$

If $m^2 + 1 \not\equiv 0 \bmod p$, then it will be invertible, and we obtain the equation

$$x^2 + 2(m^2 + 1)^{-1}m^2 + (m^2 + 1)^{-1}(m^2 - 1) \equiv 0 \mod p.$$

By construction, $x \equiv -1 \bmod p$ is one of the solutions of this equation. There is a second solution,

$$x \equiv (m^2 + 1)^{-1}(1 - m^2) \mod p.$$

By using the equation of the "line" we obtain y as

$$y \equiv (m^2 + 1)^{-1}2m \mod p.$$

Consequently, the set of solutions of the equation $x^2 + y^2 \equiv 1 \bmod p$ aside from the pair $(-1, 0)$ coincides with the collection of pairs

$$((m^2 + 1)^{-1}(1 - m^2) \bmod p, (m^2 + 1)^{-1}2m \bmod p)$$

for $1 \leq m \leq p$ subject to $m^2 + 1 \not\equiv 0 \bmod p$. If $p \equiv 3 \bmod 4$, there is no m with $p \mid m^2 + 1$. For $p \equiv 1 \bmod 4$, there are two values of m that need to be excluded. If $p = 2$, it is clear that $m = 1$ needs to be omitted. We should also not forget our seed point $(-1, 0)$. These observations mean:

$$N_p = \begin{cases} p + 1 & p \equiv 3 \bmod 4; \\ p - 1 & p \equiv 1 \bmod 4; \\ 2 & p = 2. \end{cases}$$

For p odd this formula can be written alternatively as

$$N_p = p - \left(\frac{-1}{p}\right), \tag{8.1}$$

confirming our observations.

We can also count the number of solutions of the three-variable Pythagorean equation in numbers modulo p. Set

$$N(p) = \#\{(x, y, z) \mid 1 \leq x, y, z \leq p, x^2 + y^2 \equiv z^2 \bmod p\}.$$

The quantity $N(p)$ can easily be computed knowing N_p.

First we account for solutions of $x^2 + y^2 \equiv z^2 \bmod p$ where $z \not\equiv 0 \bmod p$. For every (a, b) satisfying $a^2 + b^2 \equiv 1 \bmod p$, we have $p - 1$ solutions to $x^2 + y^2 \equiv z^2 \bmod p$, namely, the triples

$$(ac, bc, c)$$

for $1 \leq c \leq p - 1$.

Now we count the number of pairs (x, y) with $1 \leq x, y \leq p$ with $x^2 + y^2 \equiv 0 \bmod p$. If $p \equiv 3 \bmod 4$, by Lemma 5.6, there is a unique pair (p, p) that satisfies the equation. If $p \equiv 1 \bmod 4$, then we certainly have the solution (p, p), but we also have solutions (x, y) with x, y not divisible by p. In fact, there are numbers u, v such that $u \not\equiv v \bmod p$ but $u^2 + 1 \equiv v^2 + 1 \equiv 0 \bmod p$. Then we have $2(p - 1)$ additional solutions to the Pythagorean Equation:

$$(x, xu, 0), \quad 1 \leq x \leq p - 1,$$

and

$$(x, xv, 0), \quad 1 \leq x \leq p - 1.$$

This means,

$$N(p) = \begin{cases} (p-1)N_p + 1 & p \equiv 3 \bmod 4; \\ (p-1)N_p + 2(p-1) + 1 & p \equiv 1 \bmod 4. \end{cases}$$

Consequently,

$$N(p) = (p-1)N_p + \left(1 + \left(\frac{-1}{p}\right)\right)(p-1) + 1$$

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

Let us collect these findings as a proposition:

Proposition 8.1. *If p is a prime number, then*

$$N_p = \begin{cases} p - \left(\frac{-1}{p}\right) & p \text{ odd}; \\ 2 & p = 2, \end{cases}$$

and

$$N(p) = p^2.$$

We also present an alternative evaluation of $N(p)$ using Gauss sums for p odd. For x, y, whether there is a z, $z \not\equiv 0 \bmod p$, such that $x^2 + y^2 \equiv z^2 \bmod p$ is determined by $(x^2 + y^2/p)$. If there is a z, there will be exactly two of them. If on the other hand $x^2 + y^2 \equiv 0 \bmod p$, then there is a unique z, i.e., $z = p$. Hence the total number of solutions is

$$N(p) = \sum_{x,y=1}^{p} \left(1 + \left(\frac{x^2 + y^2}{p}\right)\right) = p^2 + \sum_{x,y=1}^{p} \left(\frac{x^2 + y^2}{p}\right).$$

In order to evaluate the sum, we introduce a variation of the Gauss sum introduced in Chapter 7. Recall the definition of the Gauss sum. We set $\zeta = e^{\frac{2\pi i}{p}}$ and define the pth Gauss sum by

$$\tau_p = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k.$$

For $1 \le a \le p$, we set

$$\tau_p(a) = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^{ak}$$

Lemma 8.2. *If p is prime, then*

$$\tau_p(a) = \left(\frac{a}{p}\right) \tau_p.$$

Proof. In fact, for $1 \le a \le p-1$ the identity follows from a change of variables in k. When $a = p$ the identity is equivalent to the statement that

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0.$$

We verified this last identity in the proof of Lemma 7.1. □

By the lemma,

$$\sum_{x,y=1}^{p} \left(\frac{x^2+y^2}{p}\right) = \frac{1}{\tau_p} \sum_{x,y=1}^{p} \tau_p(x^2+y^2) = \frac{1}{\tau_p} \sum_{x,y=1}^{p} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^{k(x^2+y^2)}$$

$$= \frac{1}{\tau_p} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \sum_{x,y=1}^{p} \zeta^{k(x^2+y^2)} = \frac{1}{\tau_p} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \left(\sum_{x=1}^{p} \zeta^{kx^2}\right)^2$$

If we write the inner sum $\sum_{1\le x\le p} \zeta^{kx^2}$ as $\sum_{1\le t\le p} a_t \zeta^{kt}$ then we see that

$$a_t = \begin{cases} 2 & (t/p) = 1; \\ 1 & (t/p) = 0; \\ 0 & (t/p) = -1. \end{cases}$$

Consequently,

$$\sum_{1\le x\le p} \zeta^{kx^2} = \sum_{1\le t\le p} \left(1 + \left(\frac{t}{p}\right)\right) \zeta^{kt} = \sum_{1\le t\le p} \zeta^{kt} + \sum_{1\le t\le p} \left(\frac{t}{p}\right) \zeta^{kt}$$

$$= \tau_p(k) = \left(\frac{k}{p}\right) \tau_p,$$

as for $1 \le k \le p-1$

$$\sum_{1\le t\le p} \zeta^{kt} = 0.$$

In particular, for $1 \le k \le p-1$,

$$\left(\sum_{1\le x\le p} \zeta^{kx^2}\right)^2 = \tau_p^2.$$

This means

$$\sum_{x,y=1}^{p} \left(\frac{x^2+y^2}{p}\right) = \frac{1}{\tau_p} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \tau_p^2 = \tau_p \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0,$$

by the computation in the proof of Lemma 7.1. Again, we obtain

$$N(p) = p^2.$$

The Gauss sum method described here is applicable to far more general equations than just the Pythagorean Equation. See, for example, [8, Theorem 3, Ch. 1] and [108].

8.2 Solutions modulo n for a natural number n

In this section we discuss the solutions of the Pythagorean Equation modulo a number n which is not necessarily prime. For a natural number n we set $N_n = \#S_n$ with

$$S_n = \{(x, y) \mid 1 \leq x, y \leq n, x^2 + y^2 \equiv 1 \bmod n\}.$$

Lemma 8.3. *The function N_n is multiplicative in n, i.e., if* $\gcd(m, n) = 1$, *then*

$$N_{nm} = N_n \cdot N_m.$$

Proof. We will show there is a bijection $S_{nm} \to S_n \times S_m$. This would then mean $\#S_{nm} = \#S_n \cdot \#S_m$, and that's what we are trying to prove. In order to show the existence of the bijection, we need some preparation. For $n \in \mathbb{N}$, we set

$$A_n = \{1, 2, \ldots, n\}.$$

We also let $A_n^2 = A_n \times A_n$. Observe that for each n, $S_n \subset A_n^2$.

Suppose $n \in \mathbb{N}$ and $d \mid n$. We construct a map

$$\rho_{n/d} : A_n \to A_d,$$

by defining $\rho_{n/d}(x)$, for $1 \leq x \leq n$, to be the unique $1 \leq y \leq d$ such that $x \equiv y \bmod d$. We also define a map $\rho_{n/d}^2 : A_n^2 \to A_d^2$ by defining $\rho_{n/d}^2(x, y) = (\rho_{n/d}(x), \rho_{n/d}(y))$ for $x, y \in A_n$.

We start with the observation that if $\gcd(m, n) = 1$, then the map

$$\rho_{n,m} : A_{nm} \to A_n \times A_m$$

defined by

$$\rho_{n,m}(x) = (\rho_{nm/n}(x), \rho_{nm/m}(x))$$

is a bijection. In fact, by the Chinese Remainder Theorem 2.24, if $(y_1, y_2) \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\}$, then there is a unique $1 \leq x \leq nm$ such that $\rho_{mn/n}(x) = y_1$, $\rho_{nm/m}(x) = y_2$. Clearly, $\rho_{n,m}(x) = (y_1, y_2)$. The fact that x exists and is unique means that $\rho_{n,m}$ is a bijection.

We can also define a two variable version of $\rho_{n,m}$. We define a map

$$\rho^2_{n,m} : A^2_{nm} \to A^2_n \times A^2_m$$

by defining

$$\rho^2_{n,m}(x, y) = (\rho^2_{nm/n}(x, y), \rho^2_{nm/m}(x, y)),$$

for $(x, y) \in A^2_{nm}$. The map $\rho^2_{n,m}$, too, is a bijection provided that $\gcd(n, m) = 1$.

Now consider the set $\rho^2_{n,m}(S_{nm}) \subset A^2_n \times A^2_m$ for $\gcd(n, m) = 1$. Since $\rho^2_{n,m}$ is a bijection, $\rho^2_{n,m}(S_{nm})$ is in bijection with S_{nm}, and consequently,

$$\#\rho^2_{n,m}(S_{nm}) = \#S_{nm}. \tag{8.2}$$

We claim

$$\rho^2_{n,m}(S_{nm}) = S_n \times S_m. \tag{8.3}$$

Once we establish Equation (8.3) we obtain

$$\#\rho^2_{n,m}(S_{nm}) = \#S_n \cdot \#S_m.$$

Comparing this last statement with Equation (8.2) gives the result.

In order to prove Equation (8.3), as $\rho^2_{n,m}$ is a bijection, it suffices to prove

$$(\rho^2_{n,m})^{-1}(S_n \times S_m) = S_{nm}.$$

We start with a general fact whose proof we leave as an exercise to the reader. Suppose we have we sets X, Y and a map $f : X \to Y$. Also let $A \subset X, B \subset Y$. Then $f^{-1}(B) = A$ if the following statement holds: $x \in A$ if and only if $f(x) \in B$. Because of this general statement we need to prove that $(x, y) \in S_{nm}$ if and only if $\rho^2_{n,m}(x, y) \in S_n \times S_m$. In concrete terms this means that for integers x, y, if $\gcd(n, m) = 1$, $x^2 + y^2 \equiv 1 \bmod nm$ if and only if $x^2 + y^2 \equiv 1 \bmod n$ and $x^2 + y^2 \equiv 1 \bmod m$. This last statement is completely obvious, and we are done.

□

The lemma implies that in order to determine N_n for all n, we just need to determine N_{p^α} for primes p, because then if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, we have

$$N_n = N_{p_1^{\alpha_1}} \cdots N_{p_k^{\alpha_k}}.$$

So we proceed to determine N_{p^α}. As a test case let's start with N_{p^2} for an odd prime p. The key observation is that if $x^2 + y^2 \equiv 1 \bmod p^2$, then $x^2 + y^2 \equiv 1 \bmod p$. This determines a map

$$\eta_{p^2/p} : S_{p^2} \to S_p,$$

which is simply reduction modulo p.

We now fix an element $(x_0, y_0) \in S_p$, and study the set of $(x, y) \in S_{p^2}$ that reduce to (x_0, y_0), i.e., $\eta^{-1}_{p^2/p}(x_0, y_0) \subset S_{p^2}$. Every such pair (x, y) would have to be of the form

$$(x_0 + kp, y_0 + lp)$$

for some $k, l \bmod p$. We need to have

$$(x_0 + pk)^2 + (y_0 + pk)^2 \equiv 1 \mod p^2.$$

Squaring gives

$$(x_0^2 + y_0^2 - 1) + 2p(kx_0 + ly_0) + p^2(k^2 + l^2) \equiv 0 \mod p^2,$$

or

$$(x_0^2 + y_0^2 - 1) + 2p(kx_0 + ly_0) \equiv 0 \mod p^2.$$

Since $x_0^2 + y_0^2 \equiv 1 \bmod p$, $x_0^2 + y_0^2 - 1$ is divisible by p. Dividing by p gives

$$\frac{x_0^2 + y_0^2 - 1}{p} + 2(kx_0 + ly_0) \equiv 0 \mod p.$$

Since $p \neq 2, 2$ will have a multiplicative inverse $2^{-1} \bmod p$. Then this last equation says

$$kx_0 + ly_0 \equiv -2^{-1}\frac{x_0^2 + y_0^2 - 1}{p} \mod p.$$

Since $(x_0, y_0) \neq (0, 0)$, there are p choices for (k, l) that satisfy this congruence. Consequently, we see that if $p \neq 2$, then

$$S_{p^2} = pS_p.$$

Indeed this is typical:

Lemma 8.4. *If $p \neq 2$, for each $n \geq 1$,*

$$N_{p^{n+1}} = pN_{p^n}.$$

In particular, for $n \geq 1$

$$N_{p^n} = p^n - \left(\frac{-1}{p}\right) p^{n-1}.$$

Proof. We define a map

$$S_{p^{n+1}} \to S_{p^n}$$

by reduction modulo p^n. We will see in a moment that this map is surjective. Let $(x_0, y_0) \in S_{p^n}$. We determine all (x, y) that reduce to (x_0, y_0). Every such pair (x, y) will be of the form

$$(x_0 + kp^n, y_0 + lp^n)$$

for some x, y modulo p. Then $x^2 + y^2 \equiv 1 \bmod p^{n+1}$ is equivalent to saying

$$(x_0 + kp^n)^2 + (y_0 + kp^n)^2 \equiv 1 \mod p^{n+1},$$

or

$$(x_0^2 + y_0^2 - 1) + 2p^n(kx_0 + ly_0) + p^{2n}(k^2 + l^2) \equiv 0 \mod p^{n+1}.$$

Since $2n \geq n + 1$, this last equation is equivalent to

$$(x_0^2 + y_0^2 - 1) + 2p^n(kx_0 + ly_0) \equiv 0 \mod p^{n+1}. \tag{8.4}$$

Dividing by p^n gives

$$kx_0 + ly_0 \equiv -2^{-1}\frac{x_0^2 + y_0^2 - 1}{p^n} \mod p.$$

This equation has p solutions in $k, l \bmod p$, and we are done. □

For $p = 2$ the situation is more complicated. For example, the map $S_{2^{n+1}} \to S_{2^n}$ is in general not surjective, i.e., there may be $(x_0, y_0) \in S_{2^n}$ for which there is no $(x, y) \in S_{2^{n+1}}$ satisfying $x \equiv x_0 \bmod 2^n$ and $y \equiv y_0 \bmod 2^n$. To see this in a concrete situation, let $n = 2$. Then a quick search gives

$$S_4 = \{(4, 1), (4, 3), (2, 1), (2, 3), (1, 4), (3, 4), (1, 2), (3, 2)\}.$$

Similarly we have

$$S_8 = \{(4, 1), (4, 3), (4, 5), (4, 7), (8, 1), (8, 3), (8, 5), (8, 7), (1, 4),$$

$$(3, 4), (5, 4), (7, 4), (1, 8), (3, 8), (5, 8), (7, 8)\}.$$

The image of the reduction modulo 4 map from S_8 to S_4 is

$$\{(4, 1), (4, 3), (1, 4), (3, 4)\},$$

which is visibly not all of S_4.

This in particular means that Lemma 8.4 as written is not valid for $p = 2$. One might of course try to trace the steps of the proof of Lemma 8.4 to see if any of it can be salvaged for $p = 2$. The main issue with the proof of the lemma is that in Equation (8.4) the term $2p^n(kx_0 + ly_0)$ vanishes modulo 2^{n+1} if $p = 2$, so unless $x_0^2 + y_0^2 - 1$ is already divisible by 2^{n+1}, one gets nothing. However, the key to the proof of Lemma 8.4 is that the term $2p^n(kx_0 + ly_0)$ is divisible by p^n and not p^{n+1}. In order to adapt this argument to $p = 2$, we make one small adjustment:

Lemma 8.5. *The following identity holds:*

$$N_{2^n} = \begin{cases} 2 & n = 1; \\ 2^{n+1} & n \geq 2. \end{cases}$$

Proof. That $N_2 = 2$ is obvious. We already determined N_4 and N_8. Our goal is to show that

$$N_{2^{n+1}} = 2N_{2^n}, \tag{8.5}$$

for each $n \geq 2$. Once we know this identity, an easy induction gives the lemma.

We start by obtaining some information about the structure of S_{2^n}. We define an equivalence relation on S_{2^n} by defining $(x, y) \sim (x', y')$ for $(x, y), (x', y') \in S_{2^n}$ if $x \equiv x' \bmod 2^{n-1}$ and $y \equiv y' \bmod 2^{n-1}$. Let $\mathscr{E}_1, \mathscr{E}_2, \ldots, \mathscr{E}_R$ be the equivalence classes.

Our first claim is that each equivalence class $\mathscr{E}_i$ has exactly four elements. In fact, if $(x, y), (x', y') \in S_{2^n}$ and $(x, y) \sim (x', y')$, then

$$\begin{cases} x' \equiv x + k \cdot 2^{n-1} \bmod 2^n, \\ y' \equiv y + l \cdot 2^{n-1} \bmod 2^n, \end{cases} \tag{8.6}$$

for $k, l \in \{0, 1\}$. Now, let $(x, y) \in S_{2^n}$, and for $k, l \in \{0, 1\}$ define x', y' by (8.6). We will prove that $(x', y') \in S_{2^n}$. In order to see this we compute

$$\begin{aligned} (x')^2 + (y')^2 &\equiv (x + k \cdot 2^{n-1})^2 + (y + l \cdot 2^{n-1})^2 \mod 2^n \\ &\equiv x^2 + y^2 + 2^n(k + l) + (k^2 + l^2) \cdot 2^{2(n-1)} \mod 2^n \\ &\equiv x^2 + y^2 \mod 2^n \\ &\equiv 1 \mod 2^n. \end{aligned}$$

This means that every element of the equivalence class of (x, y) is of the form (8.6), and every pair (x', y') of the form (8.6) is equivalent to (x, y). Since there are four choices for the pairs (k, l) we conclude that the equivalence class of (x, y) has four elements, as claimed. Note that this means

$$N_{2^n} = 4R. \tag{8.7}$$

For each i, fix a representative (x_i, y_i) of $\mathscr{E}_i$. The above analysis shows that

$$S_{2^n} = \bigcup_{i=1}^{R} \bigcup_{k,l \in \{0,1\}} \{(x_i + k \cdot 2^{n-1}, y_i + l \cdot 2^{n-1})\}. \tag{8.8}$$

As before we consider the reduction map

$$\eta : S_{2^{n+1}} \to S_{2^n}.$$

Let $(X, Y) \in S_{2^{n+1}}$, and $\eta(X, Y) = (x, y)$. This means that

$$X \equiv x + r \cdot 2^n, \quad Y \equiv y + s \cdot 2^n \mod 2^{n+1}.$$

Combined with (8.8) we conclude that there are $k, l, r, s \in \{0, 1\}$, and $1 \le i \le R$ such that

$$X \equiv x_i + k \cdot 2^{n-1} + r \cdot 2^n, \quad Y \equiv y_i + l \cdot 2^{n-1} + s \cdot 2^n \mod 2^{n+1}.$$

Now we examine the identity $X^2 + Y^2 \equiv 1 \bmod 2^{n+1}$ to see the types of restrictions we need on k, l, r, s. We have

$$\begin{aligned} X^2 + Y^2 &\equiv (x_i + k \cdot 2^{n-1} + r \cdot 2^n)^2 + (y_i + l \cdot 2^{n-1} + s \cdot 2^n)^2 \mod 2^{n+1} \\ &\equiv (x_i^2 + y_i^2) + 2^n(k \cdot x_i + l \cdot y_i) \mod 2^{n+1}. \end{aligned}$$

Since $X^2 + Y^2 \equiv 1 \bmod 2^{n+1}$ we conclude

$$(x_i^2 + y_i^2) + 2^n(k \cdot x_i + l \cdot y_i) \equiv 1 \mod 2^{n+1}.$$

Consequently, we need

$$k \cdot x_i + l \cdot y_i \equiv -\frac{x_i^2 + y_i^2 - 1}{2^n} \mod 2. \tag{8.9}$$

Since $x_i^2 + y_i^2 \equiv 1 \mod 2^n$, not both of x_i, y_i can be divisible by 2. As a result, there will be two pairs (k, l) with $k, l \in \{0, 1\}$ such that (8.9) is satisfied. Furthermore, once appropriate k, l are chosen, any choice of $r, s \in \{0, 1\}$ will work. Finally, $N_{2^{n+1}}$ is equal to the number of possible pairs (x_i, y_i), which is equal to R, multiplied by the number of acceptable pairs (k, l), equal to 2, multiplied by the number of all pairs (r, s), equal to 4, i.e.,

$$N_{2^{n+1}} = 2 \cdot 4 \cdot R = 8R.$$

Comparing this identity with (8.7) proves (8.5). □

Clearly this proof was much more subtle than the proof of Lemma 8.4. As noted above, what prevented us from carrying out the proof of Lemma 8.4 for $p = 2$ was the fact that in the binomial expansion

$$(x + y)^2 = x^2 + 2xy + y^2$$

the middle term is divisible by 2—and this is zero modulo 2. This suggests that if we were to consider an equation of the form

$$x^3 \equiv a \mod p^n$$

then we should run into a problem for $p = 3$, the reason being that the coefficient of x^2y in the binomial expansion

$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

is divisible by 3.

The coefficients that cause trouble in these examples are related to the derivatives of the polynomials x^2 and x^3, respectively. There is an underlying general result, Hensel's Lemma, that explains these examples. See Exercise 8.4 below for Hensel's Lemma, and Exercise 8.5 for a generalization.

Example 8.6. In this example, following the method described above, we will show that for each n, $x^2 \equiv 2 \mod 7^n$ has two solutions. We proceed by induction. If $n = 1$, then $x = 3, 4$ are the two solutions. Now suppose the assertion is true for n, and let x_n be one of the two solutions of $x^2 \equiv 2 \mod 7^n$. We will show that there is a unique $x_{n+1} \mod 7^{n+1}$ such that $x_{n+1} \equiv x_n \mod 7^n$ and $x_{n+1}^2 \equiv 2 \mod 7^{n+1}$. As before, let $x_{n+1} = x_n + k \cdot 7^n$. Since we wish to get $x_{n+1}^2 \equiv 2 \mod 7^{n+1}$ we write

$$(x_n + k \cdot 7^n)^2 \equiv x_n^2 + 2kx_n \cdot 7^n + k^2 \cdot 7^{2n} \equiv x_n^2 + 2kx_n \cdot 7^n \mod 7^{n+1}.$$

In the last step we used the fact that for $n \geq 1$, $2n \geq n+1$, and hence $7^{2n} \equiv 0 \mod 7^{n+1}$. Then we wish to have

$$x_n^2 + 2kx_n \cdot 7^n \equiv 2 \mod 7^{n+1},$$

or

$$(x_n^2 - 2) + 2kx_n \cdot 7^n \equiv 0 \mod 7^{n+1}.$$

Since $x_n^2 \equiv 2 \mod 7^n$, $7^n \mid x_n^2 - 2$. Dividing the congruence by 7^n gives

$$\frac{x_n^2 - 2}{7^n} + 2kx_n \equiv 0 \mod 7.$$

Since $7 \nmid 2x_n$, $2x_n$ is invertible modulo 7, and we obtain

$$k \equiv -(2x_n)^{-1} \cdot \frac{x_n^2 - 2}{7^n} \mod 7.$$

This means there is a unique choice for k modulo 7, and this is enough to establish the induction step.

Let us illustrate this procedure by computing the first few values of x_n. Suppose we start with $x_1 \equiv 3 \mod 7$. Write $x_2 = 3 + 7k$. We have

$$(3 + 7k)^2 \equiv 2 \mod 7^2.$$

Multiplying out gives $9 + 42k + 7^2k^2 \equiv 2 \mod 7^2$. Consequently,

$$7 + 42k \equiv 0 \mod 7^2.$$

Divide by 7 to obtain,

$$1 + 6k \equiv 0 \mod 7.$$

This gives $k = 1$, and consequently, $x_2 = 10$. We also examine x_3. Write $x_3 = x_2 + l \cdot 7^2 = 10 + l \cdot 7^2$. Then we have

$$(10 + l \cdot 7^2)^2 \equiv 100 + 2 \cdot 10 \cdot 7^2 \cdot l + 7^4 \equiv 100 + 2 \cdot 10 \cdot 7^2 \cdot l \mod 7^3.$$

Since we wish to have $x_3^2 \equiv 2 \mod 7^3$, we get

$$100 + 2 \cdot 10 \cdot 7^2 \cdot l \equiv 2 \mod 7^3.$$

Consequently, $20 \cdot 7^2 \cdot l + 98 \equiv 0 \mod 7^3$. Divide by $2 \cdot 7^2$ to obtain

$$1 + 10l \equiv 0 \mod 7.$$

We obtain $l \equiv 2 \bmod 7$. This gives $x_3 = 10 + 2 \cdot 7^2 = 108$. So, $x_1 = 3$, $x_2 = 3 + 7$, $x_3 = 3 + 7 + 2.7^2$, and the process continues. If we had started with $x_1 = 4$, we would have gotten $x_2 = 39 = 4 + 5 \cdot 7$ and $x_3 = 235 = 4 + 5 \cdot 7 + 4 \cdot 7^2$.

Exercises

8.1 Show that the equation $a_1x_1 + \cdots + a_nx_n = b$ with the a_i's integers is solvable in integers if and only if the congruence equation

$$a_1x_1 + \cdots + a_nx_n \equiv b \mod m$$

is solvable for all natural numbers m.

8.2 (✠) Numerically verify Equation (8.1) for a few small values of p.

8.3 Find an explicit formula for N_n in terms of the prime factorization of n.

8.4 Prove Hensel's Lemma: Let $f \in \mathbb{Z}[X]$, and suppose $x_1 \in \mathbb{Z}$ is such that $f(x_1) \equiv 0 \mod p$, but $f'(x_1) \not\equiv 0 \mod p$. Then for each $n \geq 1$, there is $x_n \in \mathbb{Z}$, uniquely determined modulo p^n, such that $f(x_n) \equiv 0 \mod p^n$, and $x_n \equiv x_1 \mod p$.

8.5 Here is a generalization of Hensel's Lemma: Let $f \in \mathbb{Z}[x]$. Suppose for some N and $a \in \mathbb{Z}$, we have $p^{2N+1} \mid f(a)$, $p^N \mid f'(a)$, but $p^{N+1} \nmid f'(a)$. Show that for each $M > N$ there is an $x_M \in \mathbb{Z}$, uniquely determined modulo p^M, such that $f(x_M) \equiv 0 \mod p^M$ and $x_M \equiv a \mod p^{N+1}$.

8.6 Show that the equation

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) \equiv 0 \mod m$$

is solvable for all m. This is [8, Page 3, Problem 4].

8.7 Find a homogeneous cubic polynomial in three variables x, y, z such that

$$f(x, y, z) \equiv 0 \mod 2$$

has only the zero solution.

8.8 Let ζ be a primitive pth root of unity. Let $f(x_1, \ldots, x_n)$ be a polynomial of n variables with integral coefficients. Show that the number of solutions of the congruence equation

$$f(x_1, \ldots, x_n) \equiv 0 \mod p$$

is equal to

$$\frac{1}{p} \sum_{x_1, \ldots, x_n} \sum_{x} \zeta^{xf(x_1, \ldots, x_n)}$$

where all the sums are over the set of integers $\{1, \ldots, p\}$.

8.9 Let $f(x, y) = x^3 + 7y^5$. Use the previous exercise to give an estimate the number of solutions of $f(x, y) \equiv 0 \mod p$ for a large enough prime number p. For a generalization, see [8, Ch. 1, §2].

8.10 (✠) Let $f(x) = x^2 + 2x + 7$. For each prime p, solve the equation $f(x) \equiv 0 \bmod p$, and pick representatives for the roots $0 \le v_1, v_2 \le p-1$, allowing for the possibility that v_1 and v_2 may be equal. Normalize the roots by considering $v_1/p, v_2/p \in [0, 1]$. How are these numbers distributed in the interval $[0, 1]$ as p gets large? Experiment with other polynomials, including quadratic polynomials with or without rational roots, and polynomials of higher degree.

8.11 (✠) Investigate the number of solutions of the equation $x^2 \equiv a \bmod 2^n$ for several values of a and n.

Notes

p-adic numbers

In the proofs of Lemma 8.4, Lemma 8.5, and in Example 8.6 we encountered sequences $(x_n)_{n\ge1}$ with the property that

- x_n is a congruence class modulo p^n, represented by an integer, denoted by the same letter x_n, $0 \le x_n < p^n$;
- $x_{n+1} \equiv x_n \bmod p^n$, for each $n \ge 1$.

We define a *p-adic integer* to be a sequence of integers $(x_n)_n$ satisfying these properties. We denote the set of p-adic integers by $\mathbb{Z}_p$. Note that for each $r \in \mathbb{Z}$, the ordinary set of integers, we obtain a constant sequence $\overline{r} := (r \bmod p^n)_{n\ge1} \in \mathbb{Z}_p$, showing that $\mathbb{Z}$ is naturally a subset of $\mathbb{Z}_p$. (Here $r \bmod p$ is the remainder of the division of r by p, note that for $p > r$, $r \bmod p = r$.) The set $\mathbb{Z}_p$ is a commutative ring equipped with the following operations:

$$(x_n)_{n\ge1} + (y_n)_{n\ge1} := (x_n + y_n)_{n\ge1};$$

$$(x_n)_{n\ge1} \cdot (y_n)_{n\ge1} := (x_n y_n)_{n\ge1}.$$

The zero element and the multiplicative identity of $\mathbb{Z}_p$ are given by the constant sequences $\overline{0}$ and $\overline{1}$, respectively. When there is no confusion we drop the line on top of an ordinary integer when thinking of it as a p-adic integer, e.g., we write 0 instead of $\overline{0}$.

It is not hard to see that $\mathbb{Z}_p$ has no zero divisors, i.e., if $xy = 0$, then either $x = 0$ or $y = 0$. We denote by $\mathbb{Q}_p$ the field of fractions of $\mathbb{Z}_p$, and call it *the field of p-adic numbers*. It is clear that $\mathbb{Q}_p$ contains $\mathbb{Q}$.

Let $x = (x_n) \in \mathbb{Z}_p$. Since $p^n \mid x_{n+1} - x_n$, we can write $x_{n+1} = x_n + a_n p^n$ for some $0 \le a_n < p$, and, if with analogy, we let $x_1 = a_0$, we get $x_1 = a_0$, $x_2 = a_0 + a_1 \cdot p, x_3 = a_0 + a_1 \cdot p + a_2 \cdot p^2, x_4 = a_0 + a_1 \cdot p + a_2 \cdot p^2 + a_3 \cdot p^3$, etc. We often write the p-adic integer x as a formal sum $\sum_{k=0}^{\infty} a_k \cdot p^k$, with each a_k in the

set $\{0, \ldots, p-1\}$. For example, $-1 = \sum_{k=0}^{\infty}(p-1)\cdot p^k$. If $a_0 \neq 0$, then $x = \sum_{k=0}^{\infty} a_k \cdot p^k$ is invertible in $\mathbb{Z}_p$. If we denote the set of all invertible elements in $\mathbb{Z}_p$ by $\mathbb{Z}_p^\times$, then every non-zero $x \in \mathbb{Z}_p$ can be written as $x = \varepsilon \cdot p^m$ with $\varepsilon \in \mathbb{Z}_p^\times$, $m \geq 0$. By considering quotients of such expressions, we see that every non-zero element of $\mathbb{Q}_p$ can be written as $\varepsilon \cdot p^m$ for $\varepsilon \in \mathbb{Z}_p^\times$, $m \in \mathbb{Z}$.

Exercise 8.4 can be interpreted in terms of p-adic integers in the following form, also known as Hensel's Lemma: Let $f \in \mathbb{Z}[X]$, and suppose $x_1 \in \mathbb{Z}$ is such that $f(x_1) \equiv 0 \bmod p$, but $f'(x_1) \not\equiv 0 \bmod p$. Then there is $x \in \mathbb{Z}_p$ such that $f(x) = 0$ in $\mathbb{Z}_p$. Let's examine the equation $x^2 + 1 = 0$. Clearly, this equation has no solutions in $\mathbb{Q}$. If p is an odd prime such that $p \equiv 1 \bmod 4$, then Equation (6.3) implies that the equation $x^2 + 1 \equiv 0 \bmod p$ has a solution x_1. Also if we let $f(x) = x^2 + 1$, $f'(x) = 2x$, and this implies $f'(x_1) \not\equiv 0 \bmod p$. Hensel's Lemma now implies that $x^2 + 1 = 0$ has a solution in $\mathbb{Z}_p$, and consequently in $\mathbb{Q}_p$. If on the other hand, $p \equiv 3 \bmod 4$, then since $x^2 + 1 \equiv 0 \bmod p$ has no solutions, the equation $x^2 + 1 = 0$ will have no solutions in $\mathbb{Q}_p$. It can also be shown that $x^2 + 1 = 0$ has no solutions in $\mathbb{Q}_2$.

The field of p-adic numbers can also be constructed using topology. This method resembles the way $\mathbb{R}$ is constructed from $\mathbb{Q}$ via Cauchy sequences. Recall that a Cauchy sequence of real numbers is a sequence $(x_n)_n$ such that for every $\varepsilon > 0$, there is N such that $|x_n - x_m| < \varepsilon$ for all $n, m > N$. We say Cauchy sequences $(x_n)_n$, $(y_n)_n$ are *equivalent*, and write $(x_n)_n \sim (y_n)_n$, if for all $\varepsilon > 0$, there is $N > 0$ such that $|x_n - y_m| < \varepsilon$ for all $n, m > N$. Then the field $\mathbb{R}$ can be thought of as the equivalence classes of Cauchy sequences of rational numbers modulo this equivalence relation $\sim$. Note that in this construction we did not have to specify what $|\cdot|$ is because presumably everyone is familiar with the ordinary absolute value. Let us define a new absolute value on $\mathbb{Q}$ which depends on the choice of a prime number p. For a non-zero rational number γ, we can write

$$\gamma = p^r \cdot \frac{a}{b}$$

with $r \in \mathbb{Z}$, $a, b \in \mathbb{Z}$, with $\gcd(p, ab) = 1$. Then we define $|\gamma|_p = p^{-r}$. We also define $|0|_p = 0$. Then for all rational numbers x, $|x|_p \geq 0$, and $|x|_p = 0$ if and only if $x = 0$. Also, we have a triangle inequality, $|x + y|_p \leq |x|_p + |y|_p$. In fact, we have the much stronger *ultrametric* inequality $|x + y|_p \leq \max(|x|_p, |y|_p)$.) This means that if we define $d_p(x, y) = |x - y|_p$, we obtain a metric on $\mathbb{Q}$, and it makes sense to talk about Cauchy sequences. We define a *p-Cauchy sequence* of rational numbers to be a sequence $(x_n)_n$ such that for $\varepsilon > 0$, there is N such that $|x_n - x_m|_p < \varepsilon$ for all $n, m > N$. We say the p-Cauchy sequences $(x_n)_n$, $(y_n)_n$ are *p-equivalent*, and write $(x_n)_n \sim_p (y_n)_n$, if for all $\varepsilon > 0$, there is $N > 0$ such that $|x_n - y_m|_p < \varepsilon$ for all $n, m > N$. The field $\mathbb{Q}_p$ is nothing but the p-equivalence classes of p-Cauchy sequences of rational numbers.

The beauty of the topological construction of p-adic fields is that it allows us to construct p-adic type field from other number fields. Let K be a number field as in

the Notes to Chapter 5, with $\mathcal{O}$ its ring of integers. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}$. Then if $\gamma \in K$ is non-zero, then we can let $e_{\mathfrak{p}}(\gamma)$ be the exponent with which the prime ideal $\mathfrak{p}$ occurs in the factorization of $\gamma\mathcal{O}$ as a product of prime ideals. We then define

$$|\gamma|_{\mathfrak{p}} = \#(\mathcal{O}/\mathfrak{p})^{-e_{\mathfrak{p}}(\gamma)}.$$

Here $\#(\mathcal{O}/\mathfrak{p})$ is the number of element of the quotient additive group $\mathcal{O}/\mathfrak{p}$. As before, we define $|0|_{\mathfrak{p}} = 0$. The function $|\cdot| : K \to \mathbb{R}$ gives rise to a metric, and again it makes sense to talk about Cauchy sequences and equivalence classes of Cauchy sequences. The set of equivalence classes of Cauchy sequences with respect to the metric defined by $|\cdot|_{\mathfrak{p}}$ is called the $\mathfrak{p}$-*adic field* and is denoted by $K_{\mathfrak{p}}$.

Fields of p-adic numbers have many applications in modern number theory, through their algebraic, topological, and measure theoretic properties. We refer to [41, Ch. 2, 3] for generalities regarding metric spaces and Cauchy sequences, and [8], especially Ch. 1, 2, and 4 for some applications of p-adic numbers.

Hilbert's Law of Reciprocity

Quadratic Reciprocity for fields other than $\mathbb{Q}$ is known as Hilbert Reciprocity. The formulation of this reciprocity law requires the notion of p-adic numbers introduced above. Let us explain Hilbert's formulation of the Law of Quadratic Reciprocity over $\mathbb{Q}$. Let a, b be non-zero rational numbers. For each prime p, define the *Hilbert Symbol* $(a, b)_p$ to be $+1$ if the equation $ax^2 + by^2 = z^2$ has solutions in p-adic numbers x, y, z, not all of which are zero; otherwise, we define $(a, b)_p$ to be equal to -1. We define $(a, b)_\infty$ to be $+1$ or -1 depending on whether the equation $ax^2 + by^2 = z^2$ has non-trivial solutions in real numbers, i.e., $(a, b)_\infty = -1$ if $a, b < 0$, and $+1$ otherwise. If a, b are non-zero rational numbers, then $(a, b)_p = +1$ for all but finitely many primes p. Hilbert's Law of Reciprocity for $\mathbb{Q}$ says that for all a, b non-zero rational numbers we have

$$(a, b)_\infty \cdot \prod_{p \text{ prime}} (a, b)_p = +1.$$

It is a pleasant exercise to show that this theorem implies Gauss's Law of Quadratic Reciprocity (Hint: Let $a = p, b = q$, p, q odd prime numbers). For a proof of this theorem over $\mathbb{Q}$, see Serre [44, Ch. III].

For other number fields, we need to define the generalized Hilbert symbols. Let K be a number field. First we define the analogues of $(\cdot, \cdot)_p$. For a prime ideal $\mathfrak{p}$ of K, if a, b are non-zero elements of K, then we define $(a, b)_{\mathfrak{p}} = +1$ if the equation $ax^2 + by^2 = z^2$ has non-trivial solutions in $K_{\mathfrak{p}}$, otherwise we define it to be -1. To define the analogue of $(a, b)_\infty$, we need the concept of a real embedding. A *real embedding* of K is a non-zero function $\sigma : K \to \mathbb{R}$ such that $\sigma(xy) = \sigma(x)\sigma(y)$ and

$\sigma(x+y) = \sigma(x) + \sigma(y)$ for all $x, y \in K$. For the number field K, there are only finitely many real embeddings, $\sigma_1, \sigma_2, \ldots, \sigma_r$. For example, if $K = \mathbb{Q}(\sqrt{2})$, then every element of K can be written as $u + v\sqrt{2}$ with $u, v \in \mathbb{Q}$, and the real embeddings are $\sigma_1 : u + v\sqrt{2} \mapsto u + v\sqrt{2}$ and $\sigma_2 : u + v\sqrt{2} \mapsto u - v\sqrt{2}$. For $1 \leq j \leq r$ and a, b as above, we define $(a, b)_j$ to be $+1$ if at least one of $\sigma_j(a), \sigma_j(b)$ is a positive number, otherwise we define it to be -1. If $K = \mathbb{Q}$, since $\mathbb{Q}$ has only one real embedding, $(a, b)_1 = (a, b)_\infty$ defined earlier. Hilbert's Law of Reciprocity for K is the statement that if $a, b \in K$ are non-zero, then

$$\prod_{j=1}^{r} (a, b)_j \cdot \prod_{\mathfrak{p} \text{ prime ideal}} (a, b)_{\mathfrak{p}} = +1.$$

Again, all but finitely many of the factors in this product are equal to 1, so the product makes sense. Hilbert's Law of Reciprocity for an arbitrary number field is a hard theorem. Nowadays, it is most convenient to derive this theorem from the general Artin's Law of Reciprocity which includes all the reciprocity theorems we have mentioned in this chapter. Cox [14, Ch. Two] provides a nice introduction to Artin's Law of Reciprocity. We refer to Lemmermeyer [32], especially the preface, and the references therein, for a history of these ideas.