Part III

Part III

In this, the final part of the course, we will introduce the notions of local and global viewpoints of number theory, which began with the notion of p-adic numbers. (p as usual denote a rational prime.) The basic idea is that many problems in number theory can be treated by looking at solutions mod m. We saw, say with the example of $x^2 + y^2$, that we can rule out any number $\equiv 3$ mod 4 being of the form $x^2 + y^2$.

On the other hand, suppose, for a given n, we knew a mod m solution to

$$x^2 + y^2 \equiv n \bmod m$$

for each m. Hasse's idea was that if these *local* solutions (solutions mod m for each m) are "sufficiently compatible," then we can paste them together to actually construct a *global* solution in $\mathbb{Z}$. In fact it suffices to consider the cases where $m = p^e$ is a prime power. What it means for the solutions to be sufficiently compatible means is the following. Consider $x^2 + y^2 = 244$. A solution to this in $\mathbb{Z}$ would mean in particular we have solutions mod 2 and mod 4. Here are two:

$$x^2 + y^2 \equiv 1^2 + 1^2 \equiv 0 \bmod 2, \;\; x^2 + y^2 \equiv 0^2 + 2^2 \equiv 0 \bmod 4$$

In the mod 2 solution x, y must both be odd, but in the mod 4 solution both x and y are even, so there is no way to paste together these local solutions to get a solution in integers, hence we say they are not compatible.

Essentially what the p-adic integers $\mathbb{Z}_p$ are, are the elements of

$$(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots$$

which are compatible in the above sense. In other words, a p-adic integer $x = (x_n)$ gives a congruence class x_n mod p^n for each n such that $x_{n+1} \equiv x_n$ mod p^n. We can form the field of fractions of the p-adic integers to obtain the field of p-adic number $\mathbb{Q}_p$. The advantage of this is we can use field theory, which is much stronger than ring theory, whereas we couldn't do this with a single $\mathbb{Z}/p^n\mathbb{Z}$, since $\mathbb{Z}/p^n\mathbb{Z}$ doesn't embed in a field as there are nontrivial zero divisors (unless $n = 1$). (Even though $\mathbb{Z}_p$ "contains" all of these $\mathbb{Z}/p^n\mathbb{Z}$'s, it turns out to be an integral domain.)

After discussing the p-adic numbers, we will discuss applications to quadratic forms in several variables. This naturally leads into the topic of modular forms, which is slated to be taught next year, and we will not discuss them in any detail here.

We will follow this with an introduction to adéles, which is considered a *global* way of studying things. Just like the p-adic numbers put together information mod p^n for all n, the adèles $\mathbb{A}_\mathbb{Q}$ put together $\mathbb{Q}_p$ for all p. Moreover, one can do all this over an arbitrary number field. Namely, for any number field K and prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, one can define the field $K_\mathfrak{p}$ of $\mathfrak{p}$-adic numbers. Then one define the adèles $\mathbb{A}_K$ of K, which is essentially a product of all the $K_\mathfrak{p}$'s. It turns out that $\mathbb{A}_K$ provides an alternative way to study the class group $\mathcal{C}l_K$ as well as *class field theory*, which studies the abelian extensions of K.

The adelic picture is important for several reasons, not least of which is it allows for a vast generalization of class field theory, known as *Langlands' program*, or *non-abelian class field theory.* As a special case, Langlands' program (together with Wiles' famous work) includes the famous

Taniyama–Shimura(–Weil) correspondence between elliptic curves and modular forms, which is famous for proving Fermat's last theorem. While (abelian) class field theory is more or less considered a closed book now (which is of course not to say that everything is known about abelian extensions), the Langlands' program is only in a toddler stage, and lies at the heart of the research of several faculty members here. The Langlands' program and the generalized (or grand) Riemann hypothesis are the two most important outstanding problems in both number theory and the theory of automorphic forms/representations.

Time permitting, we will give a brief introduction to abelian class field theory and Langlands' program. The second semester of next year's Modular Forms course should contain a more detailed introduction to Langlands' program.

6 p-adic numbers

Throughout this chapter p will denote a fixed prime number of $\mathbb{N}$.

In the introduction to Part III, we briefly described the p-adic integers are elements in

$$(a_n) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots$$

which are compatible in the sense that the natural map $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ maps a_{n+1} to a_n. There are several different ways to describe the p-adic numbers, which were first introduced by Hensel at the end of the 1800's. Before we proceed into the formalities of the p-adic numbers, it may be interesting to describe Hensel's original viewpoint of the p-adic numbers.

The basic idea came from an analogy with algebraic geometry. The basic premise of modern mathematics is that to study some object X, it is helpful to study functions on X. In particular, to study the complex numbers $\mathbb{C}$, one may choose to study the polynomial ring $\mathbb{C}[x]$. (The space $\mathbb{C}$ is the set of **points**, and the ring $\mathbb{C}[x]$ is called the **coordinate ring** of $\mathbb{C}$.) One of the early observations in complex algebraic geometry was that the set of maximal ideals of $\mathbb{C}[x]$ is just the set of (principal) ideals generated by a linear polynomial of the form $x - p_0$ for some point $p_0 \in \mathbb{C}$. In other words, there is a bijection between $\mathbb{C}$ and the maximal ideals of $\mathbb{C}[x]$, given by a point $p_0 \in \mathbb{C}$ corresponds to the ideal of all polynomials which vanish at p_0. Further if $f(x) \in \mathbb{C}[x]$, then we have the map

$$\begin{aligned} \mathbb{C}[x] &\to \mathbb{C}[x]/(x - p_0) \simeq \mathbb{C} \\ f(x) &\mapsto f(p_0), \end{aligned}$$

i.e., to mod out by a maximal idea $(x - p_0)$ in $\mathbb{C}[x]$, just means substituting in $x = p_0$ for a polynomial $f(x) \in \mathbb{C}[x]$, i.e., this "mod $(x - p_0)$" map $\mathbb{C}[x] \to \mathbb{C}$ just sends a polynomial $f(x)$ to its value at a point p_0.

Now instead, let's try to imagine $\mathbb{Z}$ in place of $\mathbb{C}[x]$ as a coordinate ring. What should the space of points be? Well, in analogy with the above, a good candidate is the set of maximal ideals of $\mathbb{Z}$, i.e., the set of all nonzero prime ideals (p) of $\mathbb{Z}$. In other words, if we consider the space $\mathcal{P} = \{p\mathbb{Z} : p \in \mathbb{N}\}$ of points as the natural number primes, then the coordinate ring "$\mathcal{P}[x]$," i.e., the "polynomials on the space $\mathcal{P}$," are just the integers $n \in \mathbb{Z}$. How do we evaluate a "polynomial" $n \in \mathbb{Z}$ on a point $p \in \mathcal{P}$? Just consider the map

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \\ n &\mapsto n \bmod p. \end{aligned}$$

In other words, the analogue of polynomials in one variable over $\mathbb{C}$, when we replace $\mathbb{C}$ with the set of primes $\mathcal{P}$, are the functions on $\mathcal{P}$ given by integers $n \in \mathbb{Z}$ such that $n(p) = n \bmod p$. One obvious difference is that for any $p_0 \in \mathbb{C}$, the space $\mathbb{C}[x]/(x - p_0) \simeq \mathbb{C}$, so all functions in the coordinate ring $\mathbb{C}[x]$ really map into $\mathbb{C}$. But in the case of $p \in \mathcal{P}$, the spaces $\mathbb{Z}/p\mathbb{Z}$ are all non-isomorphic, so it's harder to think of $n(p) = n \bmod p \in \mathbb{Z}/p\mathbb{Z}$ as a function, since its image lands in a different space ($\mathbb{Z}/p\mathbb{Z}$) for each p.

To go further with this analogy, one can ask about a notion of derivatives of the functions $n(p) = n \bmod p$. Observe for a polynomial $f(x) \in \mathbb{C}[x]$, we can always write $f(x)$ in the form

$$f(x) = a_0 + a_1(x - p_0) + a_2(x - p_0)^2 + \cdots + a_k(x - p_0)^k$$

where each $a_i \in \mathbb{C}$, and the m-th derivative at p_0 is just given by $m!a_m$. Similarly, for any $n \in \mathbb{Z}$, we can write n in the form

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$$

where $0 \le a_i < p$, so the m-th derivative at p should be $m!a_m$.

Since power series are such a powerful tool in function theory, Hensel wanted to apply the techniques of power series to number theory. If we work with more general functions than polynomials in $\mathbb{C}[x]$, namely analytic functions at p_0, we can write them as power series about $x = p_0$

$$f(x) = a_0 + a_1(x - p_0) + a_2(x - p_0)^2 + \cdots \in \mathbb{C}[[x]] \ \ (a_i \in \mathbb{C}).$$

Analogously, we can consider formal power series in a prime $p \in \mathcal{P}$ given by

$$n = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p \ \ (0 \le a_i < p).$$

These formal power series are the p-adic integers $\mathbb{Z}_p$. (Note $\mathbb{Z}_p$ contains $\mathbb{Z}$ by just restrict to finite sums, i.e., "polynomials" in p.)

Even more generally than analytic functions at p_0, one often considers meromorphic functions on $\mathbb{C}$ which may have a pole (go to infinity) at p_0, e.g., the Riemann zeta function $\zeta(s)$ has a pole at $s = 1$. These functions still have a series expansion at p_0, but it needs to start with some negative power of $x - p_0$. These are called Laurent series, and explicitly are of the form

$$f(x) = a_{-k}(x-p_0)^{-k} + a_{1-k}(x-p_0)^{1-k} + \cdots + a_0 + a_1(x-p_0) + a_2(x-p_0)^2 + \cdots \in \mathbb{C}((x)) \ \ (a_i \in \mathbb{C}).$$

Analogous to this, one can take formal power series in p with coefficients between 0 and p with a finite number of negative terms

$$n = a_{-k}p^{-k} + a_{1-k}p^{1-k} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Q}_p \ \ (0 \le a_i < p),$$

and this will give us the p-adic numbers $\mathbb{Q}_p$. (Note $\mathbb{Q}_p$ contains all rational numbers with denominator a power of p.)

This analogy may seem a little far fetched, and you might wonder if Hensel had one too many beers at this point, but the usefulness of the p-adic numbers allows us to recognize his ideas as brilliant, as opposed to crazy talk. We summarize the analogy in the table below, though to fully appreciate it, one should be familiar with complex function theory. Nevertheless, even if you are not, it may be helpful to refer back to this table after learning more about $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

We can now explain why $\mathbb{Z}_p$ and $\mathbb{Q}_p$ are called *local* objects, specifically, local rings and local fields. A power or Laurent series expansion of some function $f(x)$ around a point p_0 may only

Table 3: Complex functions vs. p-adic numbers

$\mathbb{C}$—space of points	$\mathcal{P} = \{p\}$—set of primes
$\mathbb{C}[x]$—polynomials over $\mathbb{C}$ $f(x) = a_0 + a_1(x - p_0) + \cdots a_k(x - p_0)^k$	$\mathbb{Z}$—“polynomials” over $\mathcal{P}$ $n = a_0 + a_1 p + \cdots + a_k p^k$
functions analytic at p_0 $f(x) = \sum_{i=0}^{\infty} a_i(x - p_0)^i$	$\mathbb{Z}_p$—p-adic integers $n = \sum_{i=0}^{\infty} a_i p^i$
functions meromorphic at p_0 $f(x) = \sum_{i=-k}^{\infty} a_i(x - p_0)^i$	$\mathbb{Q}_p$—p-adic numbers $n = \sum_{i=-k}^{\infty} a_i p^i$

converge nearby p_0, even though the function may be defined (as a meromorphic function) on all of $\mathbb{C}$. Since a power series is essentially meaningless outside its radius of convergence, power series in general only give *local* information about functions $f(x)$ (namely, near p_0). Similarly, the elements of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ will give “local” information about the prime $p \in \mathcal{P}$.

The main references I will be using for this chapter are [Neukirch] and [Serre], as these were the books I originally learned the theory from, though most if not all of this material may be found in many books on algebraic number theory, and of course any book specifically on p-adic numbers, of which there are a few. There is also a nice analytic/topological presentation in [Ramakrishnan–Valenza], which leads into adèles.

6.1 Definitions

Fix a prime $p \in \mathbb{N}$.

Definition 6.1.1. *The set of* p**-adic integers***, denoted* $\mathbb{Z}_p$*, are the formal power series of the form*

$$\sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 p + a_2 p^2 + \cdots, \ \ 0 \le a_i < p.$$

Observe the series $\sum_{i=0}^{\infty} a_i p^i$ converges if and only if it is finite, i.e., if $a_i = 0$ for all $i > k$ for some k. In this case, this finite sum is an integer, and we can get any non-negative integer this way. Accordingly we will view $\mathbb{N} \cup \{0\} \subseteq \mathbb{Z}_p$.

We can abbreviate this representation as an “infinite” base p representation of a “number:”

$$\sum_{i=0}^{\infty} a_i p^i = \cdots a_2 a_1 a_0$$

Note if the series is in fact finite, then this really is the base p representation of the corresponding integer:

$$\underbrace{a_k a_{k-1} \cdots a_2 a_1 a_0}_{\text{base } p} = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k.$$

Naively, we can think of a p-adic integer x as just a sequence $(a_i)_0^{\infty}$ of numbers between 0 and p, but the p-adic numbers will have more structure than just this. We define addition and multiplication on $\mathbb{Z}_p$ by just extending the usual addition and multiplication on base p representations of positive integers.

Example 6.1.2. *Let $x = 1 + 4 \cdot 5 + 3 \cdot 5^2, y = \sum_{i=0}^{\infty} 1 \cdot 5^i \in \mathbb{Z}_5$, and $z = 4 + 2 \cdot 5^2 + \sum_{i=3}^{\infty} 4 \cdot 5^i$. We can compute the sums*

$$\begin{array}{crc} & \cdots 0000341 & x \\ + & \cdots 1111111 & y \\ \hline & \cdots 1112002 & x+y \end{array}$$

$$\begin{array}{crc} & \cdots 0000341 & x \\ + & \cdots 4444104 & z \\ \hline & \cdots 0000000 & x+z \end{array}$$

$$\begin{array}{crc} & \cdots 1111111 & y \\ + & \cdots 4444104 & z \\ \hline & \cdots 1110220 & y+z \end{array}$$

and we can compute a product

$$\begin{array}{crc} & \cdots 1111111 & 1 \times \cdots 1111111 \\ + & \cdots 4444440 & 40 \times \cdots 1111111 \\ + & \cdots 3333300 & 300 \times \cdots 1111111 \\ \hline & \cdots 4444401 & x \cdot y \end{array}$$

Since $x + z = \cdots 00000$, we may identify x with 396 and z with -396 in $\mathbb{Z}_5$.

It is easy to see in general, that for any $x \in \mathbb{Z}_p$, the additive inverse of x (the additive zero is of course $\cdots 00000 \in \mathbb{Z}_p$) also lies in $\mathbb{Z}_p$. Hence we may regard $\mathbb{Z} \subseteq \mathbb{Z}_p$.

Exercise 6.1. *Find the 7-adic representations for -7 and -121.*

Exercise 6.2. *Let $x = 64 \in \mathbb{Z}_7$ and $y = 4 + 6 \cdot 7 + \sum_{i=2}^{\infty} 2 \cdot 7^i \in \mathbb{Z}_7$. Compute $x + y$ and $x \cdot y$.*

Exercise 6.3. *What are the p-adic representations for -1 and $\frac{1}{1-p}$ for arbitrary p?*

Proposition 6.1.3. *We have that $\mathbb{Z}_p$ is a ring with $\mathbb{Z}$ as a subring.*

The proof of this is elementary—it is just base p arithmetic with infinite sequences—but we will see another justification for this from a more algebraic description below. The statement about $\mathbb{Z}$ being a subring just means that with the identification of $\mathbb{Z} \subseteq \mathbb{Z}_p$ described above, the addition and multiplication defined on $\mathbb{Z}_p$ are compatible with those on $\mathbb{Z}$, which is evident from the way we defined them. Specifically, let ϕ_n denote the natural maps

$$\cdots \longrightarrow \mathbb{Z}/p^{n+1}\mathbb{Z} \xrightarrow{\phi_n} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \cdots \xrightarrow{\phi_2} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\phi_1} \mathbb{Z}/p\mathbb{Z}$$

Definition 6.1.4. *The* **projective limit** *(or* **inverse limit***) of $\mathbb{Z}/p^n\mathbb{Z}$ (with respect to ϕ_n) as $n \to \infty$ is*

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n) \in \prod_n \mathbb{Z}/p^n\mathbb{Z} : \phi_n(x_{n+1}) = x_n \text{ for all } n \geq 1 \right\}$$

In other words an element (x_n) of $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is a sequence of elements $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ which is compatible in the sense that $x_{n+1} \equiv x_n \mod \mathbb{Z}/p^n\mathbb{Z}$. (Recall a direct or injective limit, written $\varinjlim$, is for when we have a sequence of objects which are successively included in each other. A projective limit is for when we have a sequences of objects which are successive quotients (or *projections*) of each other. This is the natural way to construct an object X, in this case $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, such that each $\mathbb{Z}/p^n\mathbb{Z}$ is a quotient of $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$. It's of course not the smallest space X such that every $\mathbb{Z}/p^n\mathbb{Z}$ is a quotient of X—that would be $\mathbb{Z}$—but it is certainly just as natural, if not more so. If you doubt this, try to figure out how you could *construct* $\mathbb{Z}$ from the set of $\mathbb{Z}/p^n\mathbb{Z}$'s.)

The reason for the compatibility requirements was already described in the introduction to Part III. To state this reason a little differently, the idea was that we want to use $\mathbb{Z}_p$ to study solutions to equations in $\mathbb{Z}$. If we just look at $\prod_n \mathbb{Z}/p^n\mathbb{Z}$, it's not very meaningful. Note that any element $(x_n) \in \mathbb{Z}_p$ is the limit of integers $x_n \in \mathbb{Z}$, whereas a non-compatible sequence is not a limit of integers. For instance, the sequence $(1, 2, 3, 0, 0, 0, \ldots)$ in $\prod \mathbb{Z}/p^n\mathbb{Z}$

Proposition 6.1.5. *We have a bijection*

$$\mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$
$$\sum_{n=0}^{\infty} a_n p^n \mapsto (s_n)_{n=1}^{\infty}$$

where s_n is the (image in $\mathbb{Z}/p^n\mathbb{Z}$) of the n-th partial sum

$$s_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}.$$

From now on we use this bijection to identify $\mathbb{Z}_p$ with $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, and sometimes write our p-adic integers as formal power series expansions in p, and sometimes write them as sequences in the projective limit of the $\mathbb{Z}/p^n\mathbb{Z}$'s. There are some nice features of the projective limit approach.

First, there is a natural map from $\mathbb{Z} \to \mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ given by

$$a \mapsto (a \bmod p, a \bmod p^2, a \bmod p^3, \ldots) \in \prod_n \mathbb{Z}/p^n\mathbb{Z}$$

for any $a \in \mathbb{Z}$. Further we can just define addition of and multiplication of elements of $\prod \mathbb{Z}/p^n\mathbb{Z}$. Then it is immediate that $\mathbb{Z}_p$ is a ring with $\mathbb{Z}$ as a subring, i.e., the proof of Proposition 6.1.3 is immediate. (We did not actually check that the two definitions of addition and multiplication match, but this is certainly true when we restrict to the subring $\mathbb{Z}$, since $+$ and $\cdot$ are the standard operations then. Since we can approximate any $x \in \mathbb{Z}_p$ as a limit of $x_n \in \mathbb{Z}$, a density argument shows $+$ and $\cdot$ extend in a unique way to $\mathbb{Z}_p$, so the two definitions of $+$ and $\cdot$ agree.)

Example 6.1.6. *Suppose $p = 2$. Consider $n = 75 \in \mathbb{Z}$. As a power series, we can write $n = 1 \cdot 1 + 1 \cdot 2 + 1 \cdot 2^3 + 1 \cdot 2^6$. Alternatively, we can write*

$$n = (1 \bmod 2, 3 \bmod 4, 3 \bmod 8, 11 \bmod 16, 11 \bmod 64, 75 \bmod 128, 75 \bmod 256, 75 \bmod 512, \ldots)$$

as a sequence in the projective limit of $\mathbb{Z}/2^n\mathbb{Z}$. Note in the projective limit version, it's easier to write down $-n$, namely

$$-n = (-1, -3, -3, -11, -11, -75, -75, -75, -75, \ldots).$$

The usefulness of p-adic integers is that the precisely capture the answer of when an equation is solvable mod p^n for all n.

Proposition 6.1.7. *Consider a polynomial $F(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$. Then*

$$F(x_1, \ldots, x_k) \equiv 0 \bmod p^n$$

is solvable for all n if and only if

$$F(x_1, \ldots, x_k) = 0$$

is solvable in $\mathbb{Z}_p$.

Proof. ($\Leftarrow$) Suppose we have a $\mathbb{Z}_p$-solution $F(x_{,1}, \ldots, x_k) = 0$. Write $x_i = (x_{i1}, x_{i2}, x_{i3}, \ldots) \in \prod \mathbb{Z}/p^n\mathbb{Z}$. Then $F(x_{1n}, \ldots x_{kn}) \equiv 0 \bmod p^n$ for each n.

($\Rightarrow$) Let $x_{1n}, \ldots x_{kn} \in \mathbb{Z}/p^n\mathbb{Z}$ be a solution to $F(x_{1n}, \ldots, x_{kn}) \in \mathbb{Z}/p^n\mathbb{Z}$ for each n. One would like to say that $x_i = (x_{in}) \in \mathbb{Z}_p$, but the (x_{in})'s will not in general be compatible. Nevertheless, we can construct a compatible sequence of solutions.

By the (infinite) pigeonhole principle, there is a $(y_{11}, \ldots, y_{k1}) \in (\mathbb{Z}/p\mathbb{Z})^k$ such that

$$(x_{1n}, \ldots, x_{kn}) \equiv (y_{11}, \ldots, y_{k1}) \bmod p$$

for infinitely many n. Then $F(y_{11}, y_{21}, \ldots, y_{k1}) \equiv 0 \bmod p$ since any of the $(x_{1n}, \ldots, x_{kn})$ above give a solution mod p.

Similarly, there is a $(y_{12}, \ldots, y_{k2}) \in (\mathbb{Z}/p^2\mathbb{Z})^k$ such that

$$(y_{12}, \ldots, y_{k2}) \equiv (y_{11}, \ldots, y_{k1}) \bmod p$$

and

$$(x_{1n}, \ldots, x_{kn}) \equiv (y_{12}, \ldots, y_{k2}) \bmod p^2$$

for infinitely many n. Again we have $F(y_{12}, y_{22}, \ldots, y_{k2}) \equiv 0 \bmod p^2$.

We continue this ad infinitum, and set $y_i = (y_{in}) \in \prod_n \mathbb{Z}/p^n\mathbb{Z}$, so in fact each $y_i \in \mathbb{Z}_p$. Then we have $F(y_1, \ldots, y_k) = 0 \in \mathbb{Z}_p$ since this expression must be 0 in each component of $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. □

In many cases, one can reduce checking the solvabilty of an equation mod p^n to simply solvability mod p. Here is a special case.

Lemma 6.1.8. (Hensel) *Let $f(x) \in \mathbb{Z}[x]$, p a prime and $n \in \mathbb{N}$. If $p = 2$, we assume $n \geq 2$. Suppose $f(a) \equiv 0 \bmod p^n$ for some $a \in \mathbb{Z}$, but $p \nmid f'(a)$. Then for each $n \geq 1$ there is an $b \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ such that $f(b) \equiv 0 \bmod p^{n+1}$ and $b \equiv a \bmod p^n$.*

Starting with $n = 1$ (or 2 if $p = 2$) applying this inductively, we see that if we have a root a of a one-variable polynomial $f(x)$ mod p (or mod 4), it lifts to a root a_n mod p^n for all n, provided $f'(a) \neq 0$. In fact, these roots a_n can be chosen to be compatible so that $(a_n) \in \prod \mathbb{Z}/p^n\mathbb{Z}$ lies in $\mathbb{Z}_p$.

Here $f'(x)$ is the formal derivative of $f(x)$, in other words the derivative as a real polynomial.

Proof. The Taylor series for $f(x)$ (regarded as a function of a real variable x) about $x = a$ is

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)(x-a)^2}{2!} + \cdots + \frac{f^{(d)}(a)(x-a)^d}{d!}$$

where d is the degree of $f(x)$. Suppose we take x of the form $x = a + p^n y$. Then we have

$$f(x) = f(a) + f'(a)p^n y + \frac{f''(a)p^{2n}y^2}{2!} + \cdots + \frac{f^{(d)}p^{dn}y^d}{d!}$$

By induction on j, it is easy to see for $j \geq 2$ (or $j \geq 3$ if $p = 2$) that p^{n+1} divides $\frac{p^{jn}}{j!}$. In other words, we can have

$$f(x) \equiv f(a) + f'(a)p^n y \bmod p^{n+1}.$$

Since $f(a) \equiv 0 \bmod p^n$, we can write $f(a) = a_0 p^n$ so

$$f(x) \equiv a_0 p^n + f'(a)yp^n \equiv (a_0 + f'(a)y)p^n \bmod p^{n+1}.$$

Since $f'(a)$ is nonzero mod p, we can choose $0 \leq y < p$ such that $a_0 + f'(a)y \equiv 0 \bmod p$, so $f(x) \equiv 0 \bmod p^{n+1}$ and we can take $b = x$. □

There are several ways in which one can generalize Hensel's lemma, but we will not worry about these here.

Exercise 6.4. *Let $a = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$. Show a is a unit in $\mathbb{Z}_p$ if and only if $a_0 \neq 0$.*

Exercise 6.5. *Show $\mathbb{Z}_p$ is an integral domain, i.e., there are no zero divisors.*

Exercise 6.6. *Show $x^2 = 2$ has a solution in $\mathbb{Z}_7$.*

Exercise 6.7. *Write $\frac{2}{3}$ as a 5-adic integer.*

Since $\mathbb{Z}_p$ has no zero divisors, it has a field of fractions. By Exercise 6.4, we know the only nonzero elements of $\mathbb{Z}_p$ which are not invertible (w.r.t. multiplication) are the elements divisible by p, hence the field of fractions is obtained by adjoining $\frac{1}{p}$ to $\mathbb{Z}_p$, i.e., the field of fractions of $\mathbb{Z}_p$ is $\mathbb{Z}_p[\frac{1}{p}]$. Note that we can write the elements of $\mathbb{Z}_p[\frac{1}{p}]$ uniquely in the form $p^{-d}a$ where $a \in \mathbb{Z}_p$ and $d \geq 0$. If $a = a_0 + a_1 p + a_2 p^2 + \cdots$, we can write

$$p^{-d}a = a_0 p^{-d} + a_1 p^{1-d} + a_2 p^{2-d} + \cdots = \sum_{n \geq -d} a'_n p^n \tag{6.1}$$

where $a'_n = a_{n+d}$. Thus we may define the p-adic numbers as formal series starting with some finite negative power of p (called a formal Laurent series in p).

Definition 6.1.9. *The* p**-adic numbers** $\mathbb{Q}_p$ *is the set of formal Laurent series*

$$\mathbb{Q}_p = \left\{ \sum_{n \geq -d} a_n p^n : 0 \leq a_n < p, d \geq 0 \right\}.$$

We identify $\mathbb{Q}_p$ with the field of fractions $\mathbb{Z}_p[\frac{1}{p}]$ of $\mathbb{Z}_p$ as in (6.1).

Exercise 6.8. *Write $\frac{5}{12}$ as a 2-adic number.*

6.2 Valuations

If R is an integral domain, a map $|\cdot| : R \to \mathbb{R}$ which satisfies

(i) $|x| \geq 0$ with equality if and only if $x = 0$,
(ii) $|xy| = |x||y|$, and
(iii) $|x + y| \leq |x| + |y|$

is called an **absolute value** on R. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ are equivalent on R if $|\cdot|_2 = |\cdot|_1^c$ for some $c > 0$. If we have an absolute value $|\cdot|$ on R, by (ii), we know $|1 \cdot 1| = |1| = 1$. Similarly, we know $|-1|^2 = |1| = 1$, and therefore $|-x| = |x|$ for all $x \in R$.

Now a absolute value $|\cdot|$ on R makes R into a metric space with distance $d(x, y) = |x-y|$. (The fact $|-x| = |x|$ guarantees $|y-x| = |x-y|$ so the metric is symmetric, and (iii) gives the triangle inequality.) Recall that any metric space is naturally embued with a topology. Namely, a basis of open (resp. closed) neighborhoods around any point $x \in R$ is given by the set of open (resp. closed) balls $B_r(x) = \{y \in R : d(x, y) = |x - y| < r\}$ (resp. $\overline{B}_r(x) = \{y \in R : d(x, y) = |x - y| \leq r\}$) centered at x with radius $r \in \mathbb{R}$.

Ostrowski's Theorem says, that up to equivalence, every absolute value on $\mathbb{Q}$ is of one of the following types:

$|\cdot|_0$, the trivial absolute value, which is 1 on any non-zero element
$|\cdot|_\infty$, the usual absolute value on $\mathbb{R}$
$|\cdot|_p$, the **p-adic absolute value**, defined below, for any prime p.

Here the p-adic absolute value defined on $\mathbb{Q}$ is given by

$$|x| = p^{-n}$$

where $x = p^n \frac{a}{b}$ with $p \nmid a, b$. (Note any $x \in \mathbb{Q}$ can be uniquely written as $x = p^n \frac{a}{b}$ where $p \nmid a, b$ and $\frac{a}{b}$ is reduced.)

In particular, if $x \in \mathbb{Z}$ is relatively prime to p, we have $|x| = 1$. More generally, if $x \in \mathbb{Z}$, $|x| = p^{-n}$ where n is the number of times p divides x.

Note any integer $x \in \mathbb{Z}$ satisfies $|x|_p \leq 1$, and $|x|_p$ will be close to 0 if x is divisible by a high power of p. So two integers $x, y \in \mathbb{Z}$ will be close with respect to the p-adic metric if $p^n | x - y$ for a large n, i.e., if $x \equiv y \bmod p^n$ for large n.

Example 6.2.1. *Suppose $p = 2$. Then*

$$|1|_2 = 1, \ |2|_2 = \frac{1}{2}, \ |3|_2 = 1, \ |4|_2 = \frac{1}{4}, \ |5|_2 = 1, \ |6|_2 = \frac{1}{2}, \ldots$$

$$|\frac{3}{4}|_2 = 4, \ |\frac{12}{17}|_2 = \frac{1}{4}, \ |\frac{57}{36}|_2 = 4.$$

With respect to $|\cdot|_2$, the closed ball $\overline{B}_{1/2}(0)$ of radius $\frac{1}{2}$ about 0 is simply all rationals (in reduced form) with even numerator. Similarly $\overline{B}_{1/4}(0)$ of radius $\frac{1}{4}$ about 0 is simply all all rationals (in reduced form) whose numerator is congruent to $0 \bmod 4$.

Exercise 6.9. *Prove $|\cdot|_p$ is an absolute value on $\mathbb{Q}$.*

Recall, for a space R with an absolute value $|\cdot|$, one can define Cauchy sequences (x_n) in R—namely, for any $\epsilon > 0$, $|x_m - x_n| < \epsilon$ for all m, n large. One forms the completion of R with respect to $|\cdot|$ by taking equivalence classes of Cauchy sequences. Everyone knows that the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$ is $\mathbb{R}$. On the other hand, the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is $\mathbb{Q}_p$. To see this, observe that

$$\begin{aligned} x_0 &= a_{-d}p^{-d} + a_{1-d}p^{1-d} + \cdots + a_0 \\ x_1 &= a_{-d}p^{-d} + a_{1-d}p^{1-d} + \cdots + a_0 + a_1 p \\ x_2 &= a_{-d}p^{-d} + a_{1-d}p^{1-d} + \cdots + a_0 + a_1 p + a_2 p^2 \\ &\vdots \end{aligned}$$

gives a Cauchy sequence in $\mathbb{Q}$ with respect to $|\cdot|_p$. Precisely $|x_{n+1} - x_n|_p = |a_{n+1}p^{n+1}|_p = \frac{1}{p^{n+1}}$ (unless $x_{n+1} = x_n$, in which case it is of course 0). Hence these are Cauchy sequences, and their limits are just formal Laurent series in $\mathbb{Q}_p$. Hence $\mathbb{Q}_p$ is contained in the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. It is also not hard to see that any Cauchy sequence in $\mathbb{Q}_p$ converges (convince yourself).

Hence, the $\mathbb{Q}_p$'s are an arithmetic analogue of $\mathbb{R}$, just being completions of the absolute values on $\mathbb{Q}$ ($\mathbb{Q}$ is already complete with respect to the trivial absolute value—$\mathbb{Q}$ is totally disconnected with respect to $|\cdot|_0$). This approach to constructing $\mathbb{Q}_p$ gives both an absolute value and a topology on $\mathbb{Q}_p$, which are the most important things to understand about $\mathbb{Q}_p$.

Precisely, write any $x \in \mathbb{Q}_p$ as

$$x = a_m p^m + a_{m+1}p^{m+1} + \cdots, \;\; a_m \neq 0$$

for some $m \in \mathbb{Z}$. Then we define the **p-adic (exponential) valuation*** (or **ordinal**) of x to be

$$\mathrm{ord}_p(x) = m.$$

Then

$$|x|_p = p^{-m} = p^{-\mathrm{ord}_p(x)}.$$

Proposition 6.2.2. *$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \mathrm{ord}_p(x) \geq 0\} = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. In particular $\mathbb{Z}_p$ is a closed (topologically) subring of $\mathbb{Q}_p$.*

Proof. This is clear since

$$\mathbb{Z}_p = \left\{ \sum_{n \geq 0} a_n p^n \right\},$$

so $\mathbb{Z}_p$ is precisely the set of $x \in \mathbb{Q}_p$ with $\mathrm{ord}_p(x) \geq 0$. □

Corollary 6.2.3. *The group of units $\mathbb{Z}_p^\times$ of $\mathbb{Z}_p$ is*

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : \mathrm{ord}_p(x) = 0\} = \{x \in \mathbb{Q}_p : |x|_p = 1\}.$$

*One often calls absolute values $|\cdot|$ valuations on a field. Thus sometimes there is a question of whether one means the exponential valuation or the absolute value by the term "valuation." For clarity, we will reserve the term valuation for exponential valuation, and always refer to our absolute values as absolute values.

Even the term exponential valuation is somewhat confusing, as the exponential valuation is really the negative logarithm $-\log_p |\cdot|$ of the absolute value. "The exponent valuation" might be clearer terminology.

Proof. This is immediate from Exercise 6.4. □

Exercise 6.10. *Let* $p = 5$*. Determine* $\mathrm{ord}_p(x)$ *and* $|x|_p$ *for* $x = 4, 5, 10, \frac{217}{150}, \frac{60}{79}$*. Describe the (open) ball of radius* $\frac{1}{10}$ *centered around* 0 *in* $\mathbb{Q}_p$*.*

Exercise 6.11. *Let* $x \in \mathbb{Q}$ *be nonzero. Show*

$$|x|_\infty \cdot \prod_p |x|_p = 1.$$

This result will be important for us later.

Despite the fact that $\mathbb{R}$ and $\mathbb{Q}_p$ are analogous in the sense that they are both completions of nontrivial absolute values on $\mathbb{Q}$, there are a couple of fundamental ways in which the p-adic absolute value and induced topology are different from the usual absolute value and topology on $\mathbb{R}$.

Definition 6.2.4. *Let* $|\cdot|$ *be an absolute value on a field* F*. If* $|x+y| \leq \max\{|x|, |y|\}$*, we say* $|\cdot|$ *is* **nonarchimedean***. Otherwise* $|\cdot|$ *is* **archimedean***.*

The nonarchimedean triangle inequality, $|x+y| \leq \max\{|x|, |y|\}$, is called the **strong triangle inequality**.

Proposition 6.2.5. $|\cdot|_\infty$ *is archimedean but* $|\cdot|_p$ *is nonarchimedean for each* p*.*

Proof. Everyone knows $|\cdot|_\infty$ or $\mathbb{Q}$ or $\mathbb{R}$ is archimedean—this is what we are use to and the proof is just $|1+1|_\infty = 2 > 1 = \max\{|1|_\infty, |1|_\infty\}$.

Now let's show $|\cdot|_p$ is nonarchimedean on $\mathbb{Q}$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ ($\mathbb{Q}_p$ is the completion of $\mathbb{Q}$), this will imply $|\cdot|_p$ is nonarchimedean on $\mathbb{Q}_p$ also. Let $x, y \in \mathbb{Q}$. Write $x = p^m \frac{a}{b}$, $y = p^n \frac{c}{d}$, where a, b, c, d are relatively prime to p, and $m, n \in \mathbb{Z}$. Without loss of generality, assume $m \leq n$. Then we can write

$$x + y = p^m \left(\frac{a}{b} + p^{n-m} \frac{c}{d} \right) = p^m \frac{ad + p^{n-m} bc}{bd}.$$

Since $n \geq m$, the numerator on the right is an integer. The denominator are relatively prime to p since b, d are, though the numerator is possibly divisible by p (though only if $n = m$ and $p|(ad+bc)$). This means that we can write $x + y = p^{m+k} \frac{e}{f}$ where $e, f \in \mathbb{Z}$ are prime to p and $k \geq 0$. Thus

$$|x+y|_p = p^{-m-k} \leq p^{-m} = \max\left\{p^{-m}, p^{-n}\right\} = \max\{|x_p|, |y_p|\}$$

□

Notice that our proof shows that we actually have equality $|x+y|_p = \max\{|x|_p, |y|_p\}$ (since $k = 0$ above) except possibly in the case $|x|_p = |y|_p$.

Exercise 6.12. *Find two integers* $x, y \in \mathbb{Z}$ *such that*
(i) $|x|_3 = |y|_3 = \frac{1}{3}$ *but* $|x+y|_3 = \frac{1}{9}$*.*
(ii) $|x|_3 = |y|_3 = |x+y|_3 = \frac{1}{3}$*.*

Proposition 6.2.6. *Every ball* $B_r(x)$ *in* $\mathbb{Q}_p$ *is both open and closed. Thus the singleton sets in* $\mathbb{Q}_p$ *are closed.*

Using the fact that the balls are closed, one can show that $\mathbb{Q}_p$ is *totally disconnected*, i.e., its connected components are the singleton sets. However the singleton sets are not open, as that would imply $\mathbb{Q}_p$ has the discrete topology, i.e., every set would be both open and closed.

Proof. Each ball is open by definition. The following two exercises show $B_r(x)$ is also closed.

Then for any $x \in \mathbb{Q}_p$, the intersection of the closed sets $\bigcap_{r>0} B_r(x) = \{x\}$, which must be closed. □

Exercise 6.13. *Show* $B_r(x) = x + B_r(0) = \{x + y : y \in B_r(0)\}$.

Exercise 6.14. *Show that* $B_r(0)$ *is closed for any* $r \in \mathbb{R}$.

Your proof of the second exercise should make use of the fact that $|\cdot|_p$ is a *discrete* absolute value, i.e., the valuation $\mathrm{ord}_p : \mathbb{Q}_p \to \mathbb{R}$ actually has image $\mathbb{Z}$, which is a discrete subset of $\mathbb{R}$. In other words, the image of $|\cdot|_p = p^{-\mathrm{ord}_p(\cdot)}$, namely $p^{\mathbb{Z}}$, is discrete in $\mathbb{R}$ except for the limit point at 0. On the other hand, the image of the ordinary absolute value $|\cdot|_\infty$ on $\mathbb{R}$ is a *continuous* subset of $\mathbb{R}$, namely $\mathbb{R}_{\geq 0}$.

Another strange, but nice thing, about analysis on $\mathbb{Q}_p$ is that a series $\sum x_n$ converges if and only if $x_n \to 0$ in $\mathbb{Q}_p$.

While these are some very fundamental differences between $\mathbb{R}$ and $\mathbb{Q}_p$, you shouldn't feel that $\mathbb{Q}_p$ is too unnatural—just different from what you're familiar with. To see that $\mathbb{Q}_p$ isn't too strange, observe the following:

Proposition 6.2.7. $\mathbb{Q}_p$ *and* $\mathbb{R}$ *are both Hausdorff and locally compact, but not compact.*

Proof. The results for $\mathbb{R}$ should be familiar, so we will just show them for $\mathbb{Q}_p$.

Recall a space is Hausdorff if any two points can be separated by open sets. $\mathbb{Q}_p$ is Hausdorff since it is a metric space: namely if $x \neq y \in \mathbb{Q}_p$, let $d = d(x, y) = |x + y|_p$. Then for $r \leq \frac{d}{2}$, $B_r(x)$ and $B_r(y)$ are open neighborhoods of x and y which are disjoint.

Recall a Hausdorff space is locally compact if every point has a compact neighborhood. Around any $x \in \mathbb{Q}_p$, we can take the closed ball $\overline{B}_r(x)$ of radius r. This is a closed and (totally) bounded set in a complete metric space, and therefore compact. (In fact one could also take the open ball $\overline{B}_r(x)$, since we know it is closed from the previous exercise.)

Perhaps more instructively, one can show $\overline{B}_r(x)$ is sequentially compact in $\mathbb{Q}_p$, which is equivalent to compactness being a metric space. We may take a specific r if we want, say $r = 1$. Further since $\overline{B}_1(x) = x + \overline{B}_1(0)$ by the exercise above, it suffices to show $\overline{B}_1(0) = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} = \mathbb{Z}_p$ is sequentially compact. If

$$\begin{aligned} x_1 &= a_{10} + a_{11}p + a_{12}p^2 + \cdots \\ x_2 &= a_{20} + a_{21}p + a_{22}p^2 + \cdots \\ x_3 &= a_{30} + a_{31}p + a_{32}p^2 + \cdots \\ &\vdots \end{aligned}$$

is a Cauchy sequence, then for any $\epsilon > 0$, there is an $N \in \mathbb{N}$ such that $|x_m - x_n|_p < \epsilon$ for all $m, n > N$. Take $\epsilon = p^{-r}$ for $r > 0$. Then $|x_m - x_n|_p < \epsilon = p^{-r}$ means $x_m \equiv x_n \bmod p^{r+1}$, i.e., the coefficients of $1, p, p^2, \ldots, p^r$ must be the same for all x_m, x_n with $m, n > N$. Let $a_0, a_1, \ldots, a_r$

denote these coefficients. We can do this for larger and larger r (note that $a_0, \ldots, a_{r-1}$ will never change) to get a sequence (a_n), and then it is clear that the above sequence converges to

$$x = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p.$$

This provides a second proof of local compactness.

To see $\mathbb{Q}_p$ is not compact, observe the sequence $x_1 = p^{-1}$, $x_2 = p^{-2}$, $x_3 = p^{-3}, \ldots$ has no convergent subsequence. Geometrically, $|x_n| = p^n$, so this is a sequence of points getting further and further from 0, and the distance to 0 goes to infinity. $\square$

We remark that $\mathbb{Q}$, with either usual subspace topology coming from $\mathbb{R}$ or the one coming from $\mathbb{Q}_p$, is a space which is not locally compact. The reason is any open neighborhood about a point is not complete—the limit points are contained in the completion of $\mathbb{Q}$ (w.r.t. to whichever absolute value we are considering), but not in $\mathbb{Q}$. (The trivial absolute value $|\cdot|_0$ induces the discrete topology on $\mathbb{Q}$, meaning single points are open sets, so it is trivially locally compact.)

The general definition of a **local field** is a locally compact field, hence we see that $\mathbb{Q}_p$ and $\mathbb{R}$ are local fields, whereas $\mathbb{Q}$ (with the usual topology) is not.