8.1. **Motivation: Solving $x^2 \equiv a \pmod{p^n}$.** Take an odd prime p, and an integer a coprime to p. Then, as we know, $x^2 \equiv a \pmod p$ has a solution $x \in \mathbb{Z}$ iff $\left(\frac{a}{p}\right) = 1$. In this case we can suppose that $b_0^2 \equiv a \pmod p$. We claim that then $x^2 \equiv a \pmod{p^n}$ has a solution x for all $n \in \mathbb{N}$.

Assume that we have a solution x of $x^2 \equiv a \pmod{p^n}$ for some $n \geq 1$. Then x is coprime to p, so that we can find $x_1 \equiv \frac{1}{2}(x + a/x) \pmod{p^{2n}}$. (This is the standard Newton-Raphson iterative method $x_1 = x - f(x)/f'(x)$ for solving $f(x) = 0$, applied to the polynomial $f(x) = x^2 - a$, but $\pmod{p^{2n}}$ instead of in $\mathbb{R}$ or $\mathbb{C}$.) Then

$$x_1 - x = -\frac{1}{2}\left(x - \frac{a}{x}\right) = -\frac{1}{2x}\left(x^2 - a\right) \equiv 0 \pmod{p^n},$$

and

$$\begin{aligned} x_1^2 - a &= \frac{1}{4}\left(x^2 + 2a + \frac{a^2}{x^2}\right) - a \\ &= \frac{1}{4}\left(x - \frac{a}{x}\right)^2 \\ &= \frac{1}{4x^2}(x^2 - a)^2 \\ &\equiv 0 \pmod{p^{2n}} \end{aligned}$$

Thus, starting with x_0 such that $x_0^2 \equiv a \pmod{p^{2^0}}$, we get successively x_1 with $x_1^2 \equiv a \pmod{p^{2^1}}$, x_2 with $x_2^2 \equiv a \pmod{p^{2^2}}$,..., x_k with $x_k^2 \equiv a \pmod{p^{2^k}}$,..., with $x_{k+1} \equiv x_k \pmod{p^{2^k}}$. So, writing the x_i in base p, we obtain

$$\begin{aligned} x_0 &= b_0 \\ x_1 &= b_0 + b_1 p && \text{say, specified} \pmod{p^2} \\ x_2 &= b_0 + b_1 p + b_2 p^2 + b_3 p^3 && \text{say, specified} \pmod{p^4} \\ x_3 &= b_0 + b_1 p + b_2 p^2 + b_3 p^3 + b_4 p^4 + b_5 p^5 + b_6 p^6 + b_7 p^7 && \text{say, specified} \pmod{p^8}, \end{aligned}$$

and so on.

So, in any sense, is $x_\infty = \sum_{i=1}^\infty b_i p^i$ a root of $x^2 \equiv a \pmod{p^\infty}$? It turns out that, yes, it is: x_∞ is a root of $x^2 = a$ in the field $\mathbb{Q}_p$ of p-adic numbers.

8.2. **Valuations.** In order to define the fields $\mathbb{Q}_p$ of p-adic numbers for primes p, we first need to discuss valuations.

A *valuation* $|\cdot|$ on a field F is a map from F to the nonnegative real numbers satisfying

For each $x \in F$	$\lvert x\rvert = 0$ iff $x = 0$;	(ZERo)
For each $x, y \in F$	$\lvert xy\rvert = \lvert x\rvert \cdot \lvert y\rvert$;	(HOMomorphism)
For each $x, y \in F$	$\lvert x + y\rvert \leq \lvert x\rvert + \lvert y\rvert$.	(TRIangle)

If in addition

$$\text{For each } x, y \in F \qquad |x+y| \le \max(|x|, |y|), \qquad \text{(MAXimum)}$$

then $|\cdot|$ is called a *nonarchimedean* valuation. A valuation that is not nonarchimedean, i.e., for which there exist $x, y \in F$ such that $|x+y| > \max(|x|, |y|)$, is called *archimedean.* For instance the standard absolute value on $\mathbb{R}$ is archimedean because $2 = |2| = |1+1| > \max(|1|, |1|) = 1$.

Note that MAX is stronger than TRI in the sense that if MAX is true than TRI is certainly true. So to show that a valuation is nonarchimedean we only need to check that ZER, HOM and MAX hold.

Proposition 8.1. *For any valuation $|\cdot|$ on a field F we have $|1| = |-1| = 1$ and for $n \in \mathbb{N}$ (defined as the sum of n copies of the identity of F) we have $|-n| = |n|$ and $|1/n| = 1/|n|$. Further, for $n, m \in N$ we have $|n/m| = |n|/|m|$.*

Proof. We have $|1| = |1^2| = |1|^2$, using HOM, so that $|1| = 0$ or 1. But $|1| \neq 0$ by ZER, so $|1| = 1$.

Also $1 = |1| = |(-1)^2| = |-1|^2$ by HOM, so that $|-1| = 1$ since $|-1| > 0$.

Further, $|-n| = |(-1)n| = |-1| \cdot |n| = 1 \cdot |n| = |n|$, and from $n \cdot (1/n) = 1$ we get $|n| \cdot |1/n| = |1| = 1$, so that $|1/n| = 1/|n|$.

Finally, from $n/m = n \cdot (1/m)$ we get $|n/m| = |n| \cdot |1/m| = |n|/|m|$. □

8.3. **Nonarchimedean valuations.** From now on we restrict our attention to nonarchimedean valuations.

Proposition 8.2 (Principle of Domination)**.** *Suppose that we have a nonarchimedean valuation $|\cdot|$ on a field F, and that $x, y \in F$ with $|x| \neq |y|$. Then*

$$|x+y| = \max(|x|, |y|).$$

Note the equal sign in this statement!

Proof. Put $s = x + y$, and assume w.l.g. that $|x| < |y|$. Then $|s| \le \max(|x|, |y|) = |y|$, while

$$|y| = |s - x| \le \max(|s|, |-x|) = \max(|s|, |x|) = |s|,$$

since otherwise we'd have $|y| \le |x|$. Hence $|s| = |y| = \max(|x|, |y|)$. □

Corollary 8.3. *Suppose that $x_1, \dots, x_n \in F$, with $|\cdot|$ nonarchimedean. Then*

$$|x_1 + \dots, +x_n| \le \max(|x_1|, \dots, |x_n|),$$

with equality if $|x_1| > \max(|x_2, \dots, |x_n|)$.

Proof. Use induction, with the help of MAX, for the inequality. For the equality, put $x_1 = y$ and $x_2 + \dots + x_n = x$ in the Principle of Domination. □

Corollary 8.4. *For $|\cdot|$ nonarchimedean and $n \in \mathbb{Z}$ we have $|n| \le 1$.*

Proof. Apply the Corollary above with all $x_i = 1$. Then use $|-n| = |n|$. □

Lemma 8.5. *If $|\cdot|$ is a nonarchimedean valuation on F, then so is $|\cdot|^\alpha$ for any $\alpha > 0$.*

Proof. It's easily checked that ZER, HOM and MAX still hold when the valuation we start with is taken to the α-th power. $\square$

[The same does *not* apply to TRI – we need $0 < \alpha \leq 1$ for TRI to still always hold.]

8.4. **Nonarchimedean valuations on $\mathbb{Q}$.**

Corollary 8.6. *If $|\cdot|$ is a nonarchimedean valuation on $\mathbb{Q}$ with $|n| = 1$ for all $n \in \mathbb{N}$ then $|\cdot|$ is trivial, i.e., $|x| = 0$ if $x = 0$ while $|x| = 1$ if $x \neq 0$.*

Proof. We then have $|x| = 0$ by ZER, while $|n/m| = |n|/|m| = 1/1 = 1$. $\square$

We'll ignore trivial valuations from now on.

Proposition 8.7. *If $|\cdot|$ is a nonarchimedean valuation on $\mathbb{Q}$ with $|n| < 1$ for some $n \in \mathbb{N}$, then there is a prime p such that $\{n \in \mathbb{N} : |n| < 1\} = \{n \in \mathbb{N} : p \text{ divides } n\}$.*

Proof. Take the smallest positive integer n_1 such that $|n_1| < 1$. We know that $n_1 > 1$. If n_1 is composite, say $n_1 = n_2 n_3$ with $1 < n_2, n_3 < n_1$, then, by the minimality of n_1, we have $|n_2| = |n_3| = 1$, so that $|n_1| = |n_2| \cdot |n_3| = 1 \cdot 1 = 1$ by HOM, a contradiction. Hence n_1 is prime, $= p$ say.

Then for any n with $|n| < 1$ we can, by the division algorithm, write $n = qp + r$ where $0 \leq r < p$. But then $|r| = |n - qp| \leq \max(|n|, |-qp|) = \max(|n|, |-1| \cdot |q| \cdot |p|) < 1$, as $|-1| = 1$, $|q| \leq 1$ and $|p| < 1$. By the minimality of p we must have $r = 0$, so that $p \mid n$. $\square$

Next, we show that there is indeed a valuation on $\mathbb{Q}$ corresponding to each prime p. We define $|\cdot|_p$ by $|0| = 0$, $|p|_p = 1/p$ and $|n| = 1$ for $n \in \mathbb{Z}$ and coprime to p, and $|p^k n/m|_p = p^{-k}$ for n and m coprime to p. We call this the *p-adic valuation* on $\mathbb{Q}$.

Proposition 8.8. *The p-adic valuation on $\mathbb{Q}$ is indeed a valuation.*

Proof. The definition of $|\cdot|_p$ ensures that ZER and HOM hold. It remains only to check that MAX holds.

Let $x = p^k n/m$ and $y = p^{k'} n'/m'$,where $n, m, n'm'$ are all coprime to p. Suppose w.l.g. that $k \leq k'$. Then $|x|_p = |p^k|_p \cdot |n|_p / |m|_p = p^{-k}$ as $|n|_p = |m|_p = 1$ and $|p|_p = 1/p$. Similarly $|y|_p = p^{-k'} \leq |x|_p$. Hence

$$|x + y|_p = \left| \frac{p^k(nm' + p^{k'-k}n'm)}{mm'} \right|_p = \frac{p^{-k}|nm' + p^{k'-k}n'm|_p}{|mm'|_p} \leq p^{-k} = \max(|x|_p, |y|_p).$$

as $|m|_p = |m'|_p = 1$ and $|nm' + p^{k'-k}n'm|_p \leq 1$, since $nm' + p^{k'-k}n'm \in \mathbb{Z}$. $\square$

[Note that the choice of $|p|_p = 1/p$ is not particularly important, as by replacing $|\cdot|_p$ by its α-th power as in Lemma 8.5 we can make $|p|_p$ equal any number we like in the interval $(0, 1)$. But we do need to fix on a definite value!]

8.5. **The p-adic completion $\mathbb{Q}_p$ of $\mathbb{Q}$.** We first recall how to construct the real field $\mathbb{R}$ from $\mathbb{Q}$, using Cauchy sequences. Take the ordinary absolute value $|\cdot|$ on $\mathbb{Q}$, and define a *Cauchy sequence* to be a sequence $(a_n) = a_1, a_2, \ldots, a_n, \ldots$ of rational numbers with the property that for each $\varepsilon > 0$ there is an $N > 0$ such that $|a_n - a_{n'}| < \varepsilon$ for all $n, n' > N$. We define an equivalence relation on these Cauchy sequences by saying that two such sequences (a_n) and (b_n) are *equivalent* if the interlaced sequence $a_1, b_1, a_2, b_2, \ldots, a_n, b_n, \ldots$ is also a Cauchy sequence. [Essentially, this means that the sequences tend to the same limit, but as we haven't yet constructed $\mathbb{R}$, where (in general) the limit lies, we can't say that.] Having checked that this is indeed an equivalence relation on these Cauchy sequences, we define $\mathbb{R}$ to be the set of all equivalence classes of such Cauchy sequences. We represent each equivalence class by a convenient equivalence class representative; one way to do this is by the standard decimal expansion. So, the class π will be represented by the Cauchy sequence $3, 3.1, 3.14, 3.141, 3.1415, 3.14159, \ldots$, which we write as $3.14159\ldots$. Further, we can make $\mathbb{R}$ into a field by defining the sum and product of two Cauchy sequences in the obvious way, and also the reciprocal of a sequence, provided the sequence doesn't tend to 0.

[The general unique decimal representation of a real number a is

$$a = \pm 10^k (d_0 + d_1 10^{-1} + d_2 10^{-2} + \cdots + d_n 10^{-n} + \ldots),$$

where $k \in \mathbb{Z}$, and the digits d_i are in $\{0, 1, 2, \ldots, 9\}$, with $d_0 \neq 0$. Also, it is forbidden that the d_i's are all $= 9$ from some point on, as otherwise we get non-unique representations, e.g., $1 = 10^0(1.00000\ldots) = 10^{-1}(9.99999\ldots)$.]

We do the same kind of construction to define the p-adic completion $\mathbb{Q}_p$ of $\mathbb{Q}$, except that we replace the ordinary absolute value by $|\cdot|_p$ in the method to obtain *p-Cauchy sequences*. To see what we should take as the equivalence class representatives, we need the following result.

Lemma 8.9. *Any rational number m/n with $|m/n|_p = 1$ can be p-adically approximated arbitrarily closely by a positive integer. That is, for any $k \in \mathbb{N}$ there is an $N \in \mathbb{N}$ such that $|m/n - N|_p \leq p^{-k}$.*

Proof. We can assume that $|n|_p = 1$ and $|m|_p \leq 1$. We simply take $N = mn'$, where $nn' \equiv 1 \pmod{p^k}$. Then the numerator of $m/n - N$ is an integer that is divisible by p^k. $\square$

An immediate consequence of this result is that *any* rational number (i.e., dropping the $|m/n|_p = 1$ condition) can be approximated arbitrarily closely by a positive integer times a power of p. Thus one can show that any p-Cauchy sequence is equivalent to one containing only those kind of numbers. We write the positive integer N in base p, so that $p^k N = p^k(a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r)$ say, where the a_i are base-p digits $\in \{0, 1, 2, \ldots, p-1\}$, and where we can clearly assume that $a_0 \neq 0$ (as otherwise we could increase k by 1). We define $\mathbb{Q}_p$, the *p-adic numbers*, to be the set of all equivalence classes of p-Cauchy sequences of elements of $\mathbb{Q}$. Then we have the following.

Theorem 8.10. *Every nonzero element (i.e., equivalence class) in $\mathbb{Q}_p$ has an equivalence class representative of the form*

$$p^k a_0, p^k(a_0 + a_1 p), p^k(a_0 + a_1 p + a_2 p^2), \dots, p^k(a_0 + a_1 p + a_2 p^2 + \dots + a_i p^i), \dots,$$

which we write simply as

$$p^k(a_0 + a_1 p + a_2 p^2 + \dots + a_i p^i + \dots) \qquad [= p^k(\sum_{i=0}^{\infty} a_i p^i)].$$

Here, the a_i are all in $\in \{0, 1, 2, \dots, p-1\}$, with $a_0 \neq 0$.

Thus we can regard p-adic numbers as these infinite sums $p^k(\sum_{i=0}^{\infty} a_i p^i)$. We define the unary operations of negation and reciprocal, and the binary operations of addition and multiplication in the natural way, namely: apply the operation to the (rational) elements of the p-Cauchy sequence representing that number, and then choose a standard equivalence class representative (i.e., $p^k(\sum_{i=0}^{\infty} a_i p^i)$ with all $a_i \in \{0, 1, 2, \dots, p-1\}$, $a_0 \neq 0$) for the result. When we do this, we have

Theorem 8.11. *With these operations, $\mathbb{Q}_p$ is a field, the field of p-adic numbers, and the p-adic valuation $|\cdot|_p$ can be extended from $\mathbb{Q}$ to $\mathbb{Q}_p$ by defining $|a|_p = p^{-k}$ when $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$. Again, the a_i are all in $\in \{0, 1, 2, \dots, p-1\}$, with $a_0 \neq 0$.*

We shall skip over the tedious details that need to be checked to prove these two theorems.

Note that, like $\mathbb{R}$, $\mathbb{Q}_p$ is an uncountable field of characteristic 0 (quite unlike $\mathbb{F}_p$, which is a finite field of characteristic p).

We define a *p-adic integer* to be an p-adic number a with $|a|_p \leq 1$, and $\mathbb{Z}_p$ to be the set of all p-adic integers.

Proposition 8.12. *With the arithmetic operations inherited from $\mathbb{Q}_p$, the set $\mathbb{Z}_p$ is a ring.*

Proof. This is simply because if a and $a' \in \mathbb{Z}_p$, then $|a|_p \leq 1$ and $|a'|_p \leq 1$, so that

$$\begin{aligned} |a + a'|_p &\leq \max(|a|_p, |a'|_p) && \leq 1 && \text{by MAX ;} \\ |a \cdot a'|_p &= |a|_p \cdot |a'|_p && \leq 1 && \text{by HOM ,} \end{aligned}$$

showing that $\mathbb{Z}_p$ is closed under both addition and multiplication, and so is a ring. $\square$

An p-adic number a is called a *p-adic unit* if $|a|_p = 1$. Then $k = 0$ so that $a = \sum_{i=0}^{\infty} a_i p^i$ with all $a_i \in \{0, 1, 2, \dots, p-1\}$ and $a_0 \neq 0$. The set of all p-adic units is a multiplicative subgroup of the multiplicative group $\mathbb{Q}_p^\times = \mathbb{Q}_p \setminus \{0\}$. This is because if $|a|_p = 1$ then $|1/a|_p = 1/|a|_p = 1$, so that $1/a$ is also a unit.

8.6. **Calculating in $\mathbb{Q}_p$.**

8.6.1. *Negation.* If $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$, then

$$-a = p^k\left((p - a_0) + \sum_{i=1}^{\infty}(p - 1 - a_i)p^i\right),$$

as can be checked by adding a to $-a$ (and getting 0!). Note that from all $a_i \in \{0, 1, 2, \dots, p-1\}$ and $a_0 \neq 0$ we have that the same applies to the digits of $-a$.

8.6.2. *Reciprocals.* If $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$, then

$$\frac{1}{a} = p^{-k}(a_0' + a_1' p + \cdots + a_i' p^i + \dots)$$

say, where for any i the first i digits $a_0', a_1', \dots, a_i'$ can be calculated as follows: Putting $a_0 + a_1 p + \cdots + a_i p^i = N$, calculate $N' \in \mathbb{N}$ with $N' < p^{i+1}$ such that $NN' \equiv 1 \pmod{p^{i+1}}$. Then writing N' in base p as $N' = a_0' + a_1' p + \cdots + a_i' p^i$ gives $a_0', a_1', \dots, a_i'$.

8.6.3. *Addition and multiplication.* If $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$ and $a' = p^k(\sum_{i=0}^{\infty} a_i' p^i)$ (same k) then $a + a' = p^k((a_0 + a_0') + (a_1 + a_1')p + \cdots + (a_i + a_i')p^i + \dots)$, where then 'carrying' needs to be performed to get the digits of $a + a'$ into $\{0, 1, 2, \dots, p-1\}$. If $a' = p^{k'}(\sum_{i=0}^{\infty} a_i' p^i)$ with $k' < k$ then we can pad the expansion of a' with initial zeros so that we can again assume that $k' = k$, at the expense of no longer having a_0' nonzero. Then addition can be done as above.

Multiplication is similar: multiplying $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$ by $a' = p^{k'}(\sum_{i=0}^{\infty} a_i' p^i)$ gives

$$a \cdot a' = p^{k+k'}(a_0 a_0' + (a_1 a_0' + a_0 a_1')p + \cdots + (\sum_{j=0}^{i} a_j a_{i-j}')p^i + \dots),$$

where then this expression can be put into standard form by carrying.

8.7. **Expressing rationals as p-adic numbers.** Any nonzero rational can clearly be written as $\pm p^k m/n$, where m, n are positive integers coprime to p (and to each other), and $k \in \mathbb{Z}$. It's clearly enough to express $\pm m/n$ as a p-adic number $a_0 + a_1 p + \dots$, as then $\pm p^k m/n = p^k(a_0 + a_1 p + \dots)$.

8.7.1. *Representating $-m/n$, where $0 < m < n$.* We have the following result.

Proposition 8.13. *Put $e = \varphi(n)$. Suppose that m and n are coprime to p, with $0 < m < n$, and that the integer*

$$m\frac{p^e - 1}{n} \qquad \textit{is written as} \qquad d_0 + d_1 p + \cdots + d_{e-1}p^{e-1}$$

in base p. Then

$$-\frac{m}{n} = d_0 + d_1 p + \cdots + d_{e-1}p^{e-1} + d_0 p^e + d_1 p^{e+1} + \cdots + d_{e-1}p^{2e-1} + d_0 p^{2e} + d_1 p^{2e+1} + \dots.$$

Proof. We know that $\frac{p^e-1}{n}$ is an integer, by Euler's Theorem. Hence

$$-\frac{m}{n} = \frac{m\frac{p^e-1}{n}}{1-p^e} = (d_0 + d_1 p + \cdots + d_{e-1}p^{e-1})(1 + p^e + p^{2e} + \ldots),$$

which gives the result. □

In the above proof, we needed $m < n$ so that $m\frac{p^e-1}{n} < p^e$, and so had a representation $d_0 + d_1 p + \cdots + d_{e-1}p^{e-1}$.

8.7.2. *The case m/n, where $0 < m < n$.* For this case, first write $-m/n = u/(1-p^e)$, where, as above, $u = m \cdot \frac{p^e-1}{n}$. Then

$$\frac{m}{n} = \frac{-u}{1-p^e} = 1 + \frac{p^e - 1 - u}{1-p^e} = 1 + \frac{u'}{1-p^e},$$

where $u' = p^e - 1 - u$ and $0 \le u' < p^e$. Thus we just have to add 1 to the repeating p-adic integer $u' + u'p^e + u'p^{2e} + \ldots$.

Example What is $1/7$ in $\mathbb{Q}_5$?
From $5^6 \equiv 1 \pmod 7$ (Fermat), and $(5^6-1)/7 = 2232$, we have

$$\begin{aligned}
-\frac{1}{7} &= \frac{2232}{1-5^6}\\
&= \frac{2 + 1\cdot 5 + 4\cdot 5^2 + 2\cdot 5^3 + 3\cdot 5^4}{1-5^6}\\
&= (21423)(1 + 5^6 + 5^{12} + \ldots)\\
&= 214230\,214230\,214230\,214230\,214230\ldots.
\end{aligned}$$

Hence

$$\frac{1}{7} = 330214\,230214\,230214\,230214\,230214\,230214\ldots,$$

which is a way of writing $3 + 3\cdot 5^1 + 0\cdot 5^2 + 2\cdot 5^3 + \ldots$.

8.8. **Taking square roots in $\mathbb{Q}_p$.**

8.8.1. *The case of p odd.* First consider a p-adic unit $a = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$, where p is odd. Which such a have a square root in $\mathbb{Q}_p$? Well, if $a = b^2$, where $b = b_0 + b_1 p + b_2 p^2 + \cdots \in \mathbb{Z}_p$, then, working modulo p we see that $a_0 \equiv b_0^2 \pmod p$, so that a_0 must be a quadratic residue $\pmod p$. In this case the method in Section 8.1 will construct b. Note that if at any stage you are trying to construct $b \pmod n$ then you only need to specify $a \pmod n$, so that you can always work with rational integers rather than with p-adic integers.

On the other hand, if a_0 is a quadratic nonresidue, then a has no square root in $\mathbb{Q}_p$.

Example. Computing $\sqrt{6}$ in $\mathbb{Q}_5$. While the algorithm given in the introduction to this chapter is a good way to compute square roots by computer, it is not easy to use by hand. Here is a simple way to compute square roots digit-by-digit, by hand: Write $\sqrt{6} = b_0 + b_1 \cdot 5^1 + b_2 \cdot 5^2 + \dots$. Then, squaring and working mod 5, we have $b_0^2 \equiv 1 \pmod 5$, so that $b_0 = 1$ or 4. Take $b_0 = 1$ (4 will give the other square root, which is minus the one we're computing.)

Next, working mod 5^2, we have

$$\begin{aligned} 6 &\equiv (1 + b_1 \cdot 5)^2 \pmod{5^2} \\ 6 &\equiv 1 + 10b_1 \pmod{5^2} \\ 1 &\equiv 2b_1 \pmod 5, \end{aligned}$$

giving $b_1 = 3$. Doing the same thing mod 5^3 we have

$$\begin{aligned} 6 &\equiv (1 + 3 \cdot 5 + b_2 \cdot 5^2)^2 \pmod{5^3} \\ 6 &\equiv 16^2 + 32b_2 \cdot 5^2 \pmod{5^3} \\ -250 &\equiv 32b_2 \cdot 5^2 \pmod{5^3} \\ 0 &\equiv 32b_2 \pmod 5, \end{aligned}$$

giving $b_2 = 0$. Continuing mod 5^4, we get $b_3 = 4$, so that $\sqrt{6} = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + \dots$.

Next, consider a general p-adic number $a = p^k(a_0 + a_1 p + \dots)$. If $a = b^2$, then $|a|_p = |b|_p^2$, so that $|b|_p = |a|_p^{1/2} = p^{-k/2}$. But valuations of elements of $\mathbb{Q}_p$ are integer powers of p, so that if k is odd then $b \notin \mathbb{Q}_p$. But if k is even, there is no problem, and a will have a square root $b = p^{k/2}(b_0 + b_1 p + \dots) \in \mathbb{Q}_p$ iff a_0 is a quadratic residue $\pmod p$.

8.8.2. *The case of p even.* Consider a 2-adic unit $a = 1 + a_1 2 + a_2 2^2 + \dots \in \mathbb{Z}_2$. If $a = b^2$, where $b = b_0 + b_1 2^1 + b_2 2^2 + \dots \in \mathbb{Z}_2$, working modulo 8, we have $b^2 \equiv 1 \pmod 8$, so that we must have $a \equiv 1 \pmod 8$, giving $a_1 = a_2 = 0$. When this holds, the construction of Section 8.1 will again construct b. On the other hand, if $a \not\equiv 1 \pmod 8$, then a has no square root in $\mathbb{Q}_2$.

For a general 2-adic number $a = 2^k(1 + a_1 2 + a_2 2^2 + \dots)$, we see that, similarly to the case of p odd, a will have a square root in $\mathbb{Q}_2$ iff k is even and $a_1 = a_2 = 0$.

8.9. **The Local-Global Principle.** The fields $\mathbb{Q}_p$ (p prime) and $\mathbb{R}$, and their finite extensions, are examples of *local fields.* These are *complete* fields, because they contain all their limit points. On the other hand, $\mathbb{Q}$ and its finite extensions are called *number fields* and are examples of *global fields.* [Other examples of global and local fields are the fields $\mathbb{F}(x)$ of rational functions over a finite field $\mathbb{F}$ (global) and their completions with respect to the valuations on them (local).] One associates to a global field the local fields obtained by taking the completions of the field with respect to each valuation on that field.

Suppose that you are interested in whether an equation $f(x, y) = 0$ has a solution x, y in rational numbers. Clearly, if the equation has no solution in $\mathbb{R}$, or in some $\mathbb{Q}_p$, then, since these fields contain $\mathbb{Q}$, the equation has no solution on $\mathbb{Q}$ either.

For example, the equation $x^2+y^2=-1$ has no solution in $\mathbb{Q}$ because it has no solution in $\mathbb{R}$. The equation $x^2+3y^2=2$ has no solution in $\mathbb{Q}$ because it has no solution in $\mathbb{Q}_3$, because 2 is a quadratic nonresidue of 3.

The Local-Global (or Hasse-Minkowski) Principle is said to hold for a class of equations (over $\mathbb{Q}$, say) if, whenever an equation in that class has a solution in each of its completions, it has a solution in $\mathbb{Q}$. This principle holds, in particular, for quadratic forms. Thus for such forms in three variables, we have the following result.

Theorem 8.14. *Let a, b, c be nonzero integers, squarefree, pairwise coprime and not all of the same sign. Then the equation*

$$ax^2+by^2+cz^2=0 \tag{1}$$

has a nonzero solution $(x, y, z) \in \mathbb{Z}^3$ iff
$-bc$ is a quadratic residue of a; i.e. the equation $x^2 \equiv -bc \pmod{a}$ has a solution x;
$-ca$ is a quadratic residue of b;
$-ab$ is a quadratic residue of c.

(Won't prove.) The first of these conditions is necessary and sufficient for (1) to have a solution in $\mathbb{Q}_p$ for each odd prime dividing a. Similarly for the other two conditions. The condition that a, b, c are not all of the same sign is clearly necessary and sufficent that (1) has a solution in $\mathbb{R}$. But what about a condition for a solution in $\mathbb{Q}_2$?

8.9.1. *Hilbert symbols.* It turns out that we don't need to consider solutions in $\mathbb{Q}_2$, because if a quadratic form has no solution in $\mathbb{Q}$ then it has no solution in a positive, even number (so, at least 2!) of its completions. Hence, if we've checked that it has a solution in all its completions except one, it must in fact have a solution in all its completions, and so have a solution in $\mathbb{Q}$. This is best illustrated by using Hilbert symbols and Hilbert's Reciprocity Law.

For $a, b \in \mathbb{Q}$ the Hilbert symbol $(a, b)_p$, where p is a prime or ∞, and $\mathbb{Q}_\infty = \mathbb{R}$, is defined by

$$(a,b)_p = \begin{cases} 1 & \text{if } ax^2+by^2=z^2 \text{ has a nonzero solution in } \mathbb{Q}_p; \\ -1 & \text{otherwise.} \end{cases}$$

Hilbert's Reciprocity Law says that $\prod_p (a,b)_p = 1$. (Won't prove; it is, however, essentially equivalent to the Law of Quadratic Reciprocity.) Hence, a finite, even number of $(a, b)_p$ (p a prime or ∞) are equal to -1.

8.10. **Nonisomorphism of $\mathbb{Q}_p$ and $\mathbb{Q}_q$.** When one writes rational numbers to any (integer) base $b \geq 2$, and then forms the completion with respect to the usual absolute value $|\cdot|$, one obtains the real numbers $\mathbb{R}$, (though maybe written in base b). Thus the field obtained ($\mathbb{R}$) is independent of b. Furthermore, b needn't be prime.

However, when completing $\mathbb{Q}$ (in whatever base) with respect to the p-adic valuation to obtain $\mathbb{Q}_p$, the field obtained *does* depend on p, as one might expect, since a different valuation is being used for each p. One can, however, prove this directly:

Theorem 8.15. *Take p and q to be two distinct primes. Then $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic.*

Proof. We can assume that p is odd. Suppose first that q is also odd. Let n be a quadratic nonresidue $\pmod q$. Then using the Chinese Remainder Theorem we can find $k, \ell \in \mathbb{N}$ with $1+kp = n+\ell q$. Hence, for $a = 1+kp$ we have $\left(\frac{a}{p}\right) = \left(\frac{1}{p}\right) = 1$ while $\left(\frac{a}{q}\right) = \left(\frac{n}{q}\right) = -1$. Hence, by the results of Subsection 8.8 we see that $\sqrt{a} \in \mathbb{Q}_p$ but $\sqrt{a} \notin \mathbb{Q}_q$. Thus, if there were an isomorphism $\phi : \mathbb{Q}_p \to \mathbb{Q}_q$ then we'd have

$$\phi(\sqrt{a})^2 = \phi(\sqrt{a}^2) = \phi(a) = \phi(1 + 1 + \cdots + 1) = a,$$

so that $\phi(\sqrt{a})$ *would* be a square root of a in $\mathbb{Q}_q$, a contradiction.

Similarly, if $q = 2$ then we can find $a = 1 + kp = 3 + 4\ell$, so that $\sqrt{a} \in \mathbb{Q}_p$ again, but $\sqrt{a} \notin \mathbb{Q}_2$. so the same argument applies. $\square$

Note that for any integer $b \geq 2$ one can, in fact, define the ring of b-adic numbers, which consists of numbers $p^k(a_0 + a_1 b + a_2 b^2 + \cdots + a_i b^i + \dots)$, where $k \in \mathbb{Z}$ and all $a_i \in \{0, 1, 2, \dots, b-1\}$. However, if b is composite, this ring has nonzero zero divisors (nonzero numbers a, a' such that $aa' = 0$), so is not a field. See problem sheet 5 for the example $b = 6$.