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 $a_0 \ne 0$, 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 $\varepsilon \in \mathbb{Z}_p^\times$, $m \ge 0$. 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, $|x|_p \ge 0$, and $|x|_p = 0$ if and only if $x = 0$. Also, we have a triangle inequality, $|x + y|_p \le |x|_p + |y|_p$. In fact, we have the much stronger *ultrametric* inequality $|x + y|_p \le \max(|x|_p, |y|_p)$.) 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