MODEL ANSWERS TO THE FIFTH HOMEWORK

3.5.9. It is clear that $\mathcal{O}_p$ is a ring. Suppose that α and β are two non-zero p-adic integers. Then

$$\alpha = p^m(a_0 + a_1p^2 + \dots) \qquad \text{and} \qquad \beta = p^n(b_0 + b_1p^2 + \dots),$$

where a_0 and b_0 are non-zero. In this case

$$\alpha\beta = p^{n+m}(c_0 + c_1p + \dots),$$

where $c_0 \equiv a_0b_0 \mod p$. In particular $c_0 \neq 0$, so that $\mathcal{O}_p$ has no zero divisors.

If $|\alpha|_p = 1$ then

$$\alpha = a_0 + a_1p + \dots,$$

where $a_0 \neq 0$. It follows that we may find b_0 such that $a_0b_0 \equiv 1 \mod p$. Note that

$$(a_0 + a_1p + \dots + a_mp^m) \cdot b_0 \equiv 1 \mod p,$$

for all n. Therefore we can solve the equation

$$(a_0 + a_1p + \dots + a_mp^m)x \equiv 1 \mod p^n$$

for all m And n. This defines

$$\beta \in \mathcal{O}_p \qquad \text{such that} \qquad \alpha\beta = 1.$$

Hence α is a unit. Conversely, if

$$\alpha\beta = 1$$

then

$$\nu_p(\alpha) + \nu_p(\beta) = 0,$$

so that $\nu_p(\alpha) = 0$ and

$$|\alpha|_p = 1.$$

3.5.10. Suppose that

$$a = \frac{b}{c}$$

is a non-zero rational number. As the norm is multiplicative, we may assume that $c = 1$, so that $a \in \mathbb{Z}$ is a non-zero integer. We may also assume that $a > 0$ so that a is a natural number. As the norm is multiplicative, we may assume that $a = p$ is a prime. In this case

$$|a|_q = \begin{cases} \frac{1}{p} & \text{if } q = p \\ 1 & \text{otherwise.} \end{cases}$$

As $|a| = p$ the result follows.
3.5.11. Consider the p-adic integer

$$\alpha = 1 + p^k + p^{2k} + \dots.$$

We have

$$\begin{aligned}\alpha - 1 &= p^k + p^{2k} + p^{3k} + \dots \\ &= p^k(1 + p^k + p^{2k} + \dots) \\ &= p^k \alpha.\end{aligned}$$

Thus

$$\alpha = \frac{-1}{p^k - 1} \in \mathbb{Q}.$$

Suppose that

$$\alpha = p^n(a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \dots).$$

We may assume that $n = 0$ so that α is a p-adic integer. If $a_0, a_1, a_2, \dots$ is eventually periodic then we can find $b_1, b_2, \dots, b_k$ and l such that if $n > l$ then

$$a_n = b_r,$$

where r is the remainder after dividing k into $n - l$. It follows that

$$\alpha = \alpha_0 + \alpha_1 + \dots + \alpha_k,$$

where

$$\begin{aligned}\alpha_0 &= a_0 + a_1 p + \dots + a_l p^l \in \mathbb{Z} \\ \alpha_1 &= b_1 p^{l+1}(1 + p^k + p^{2k} + \dots) \\ \alpha_2 &= b_2 p^{l+2}(1 + p^k + p^{2k} + \dots) \\ &\vdots \\ \alpha_k &= b_k p^{l+k}(1 + p^k + p^{2k} + \dots).\end{aligned}$$

By what we have already proved, every term $\alpha_0, \alpha_1, \dots, \alpha_k$ is a rational number and so α is a rational number.
Now suppose that $\alpha = a/b$ is a rational number. There is no harm in assuming that $a = \pm 1$, since multiplying α by an integer preserves periodicity.
Note that Euler's theorem implies that

$$p^{\varphi(b)} \equiv 1 \mod b,$$

so that b divides $p^k - 1$, where $k = \varphi(b)$. It follows that

$$\frac{-1}{b} = \frac{c}{p^k - 1},$$

where c is an integer. But we already saw that the expression on the right has an eventually periodic expression as a p-number.
3.5.12. One direction is clear; if the series converges the terms must be going to zero, so that

$$\lim_{k \to \infty} |a_k|_p = 0.$$

Now suppose that

$$\lim_{k \to \infty} |a_k|_p = 0.$$

Pick $\epsilon > 0$. Then we may find k_0 such that if $k \geq k_0$ then

$$|a_k|_p < \epsilon.$$

But then

$$\begin{aligned} |\sum_{k_0 \leq k \leq k_1} a_k|_p &= \max_{k_0 \leq k \leq k_1} (|a_k|_p) \\ &< \epsilon. \end{aligned}$$

Thus the series converges, as the partial sums are going to zero.
3.5.13. Immediate from 3.5.12.
8.2.1. First note that the last result is false as stated. Consider

$$x^2 + y^2 = 2.$$

This has the integral solution $x = y = 1$. We have

$$p = -4 \qquad q = 0 \qquad r = 8 \qquad \text{so that} \qquad k = -32.$$

k is non-zero and p is not a square and yet

$$x^2 + y^2 = 2$$

has only finitely many solutions with bounded denominators.
Consider the equation:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

If we consider the LHS as a polynomial in x, then we get the equation

$$ax^2 + (by + d)x + (cy^2 + ey + f) = 0.$$

This has a rational solution in x provided

$$(by + d)^2 - 4a(cy^2 + ey + f)$$

is a square. Expanding as a polynomial in y we get

$$(b^2 - 4ac)y^2 + (2bd - 4ae)y + (d^2 - 4af).$$

This reduces to

$$py^2 + 2qy + r.$$

We want this to be a square, so we introduce another variable z. We have

$$z^2 = py^2 + 2qy + r.$$

Rearranging, we get

$$py^2 + 2qy + (r - z^2) = 0.$$

For this to have a solution we must have

$$4q^2 - 4p(r - z^2)$$

is a square. We introduce another variable w. Thus

$$w^2 = q^2 - pr + pz^2.$$

Rearranging we get

$$w^2 - pz^2 = k.$$

Suppose we have an integer solution w and z. It follows that

$$py^2 + 2qy + (r - z^2) = 0$$

has a rational solution. By the quadratic formula, it follows that there is a solution with $2py \in \mathbb{Z}$. As the equation

$$ax^2 + (by + d)x + (cy^2 + ey + f) = 0$$

has a rational solution, whose discriminant is an integer. Again by the quadratic formula it follows that there is a solution such that $4apx$ is an integer.

Conversely suppose we have rational numbers x and y such that $4apx$ and $2py$ are integers. Then we we get a rational solution to the equation

$$w^2 - pz^2 = k.$$

As the quadratic equation

$$py^2 + 2qy + (r - z^2) = 0$$

has a solution such that $2py$ is an integer, it must have a discriminant which is a square. As the discriminant is also an integer, it follows that z is an integer. But then w is an integer, as its square is an integer.

Suppose that $k \neq 0$ and $p > 0$ is not a square. Then there are infinitely many units. As we have one solution this equation then has infinitely many solutions.

8.2.2. We follow the notation of 8.2.1. We have

$$\begin{aligned}
p &= 6^2 - 4 \cdot 1 \cdot -4 \\
&= 36 + 16 \\
&= 52, \\
q &= 6 \cdot -4 - 2 \cdot -12 \\
&= -24 + 24 \\
&= 0, \\
r &= 4^2 - 4 \cdot -19 \\
&= 4(4 + 19) \\
&= 92, \\
k &= -52 \cdot 92 \\
&= -2^4 \cdot 13 \cdot 23 \\
&= -4784.
\end{aligned}$$

Using 8.2.1, we have to solve

$$w^2 - 52z^2 = -4784.$$

If we rewrite this equation as

$$w^2 = 2^2 \cdot 13(z^2 - 4 \cdot 23)$$

it is clear we have to choose z so that $z^2 - 4 \cdot 23$ is divisible by 13. Trial and error gives $z = 12$. In this case

$$144 - 4 \cdot 23 = 52 = 4 \cdot 13.$$

Thus

$$z = 12 \qquad \text{and} \qquad w = 4 \cdot 13 = 52.$$

We have to solve

$$py^2 + 2qy + r = z^2.$$

This gives

$$52y^2 + 92 = 144,$$

so that $y^2 = 1$. Thus $y = \pm 1$. This gives

$$x^2 + 2x - 35 = 0 \qquad \text{and} \qquad x^2 - 10x - 11 = 0.$$

This gives integral solutions

$$(x, y) = (5, 1) \qquad (-7, 1) \qquad (11, -1) \qquad \text{and} \qquad (-1, -1).$$

8.2.3. We look for the fundamental solution $\delta = x + y\sqrt{d}$ by trial and error. Reducing modulo 2, we know that x has to be odd and reducing modulo 4, we know that y has to be even. If we try $x = 3$ and $y = 2$ we get a solution and this is clearly the fundamental solution,

$$\delta = 3 + 2\sqrt{2}.$$

It follows that the general solution is

$$\pm(3 + 2\sqrt{2})^n.$$

8.2.5. Consider the equation

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

It has one solution $x = y = 1$ and so it has infinitely many in the same class. Hence it has infinitely many solutions with x and $y > 0$. We have

$$|x - y\sqrt{2}| = \frac{1}{|x + y\sqrt{2}|}$$

which goes to zero as y goes to infinity. Thus

$$\begin{aligned} |x + y\sqrt{2}| &= |x - y\sqrt{2} + 2y\sqrt{2}| \\ &\leq |x - y\sqrt{2}| + 2y\sqrt{2}. \end{aligned}$$

Thus

$$y|x - y\sqrt{2}| \leq \frac{1+\epsilon}{2\sqrt{2}}.$$

Let $u = \llcorner n\sqrt{2} \lrcorner$ and $v = n$. Note that

$$u^2 - 2v^2 < 0$$

and if

$$x^2 - 2y^2 < 0 \qquad \text{where} \qquad x > 0, y = n$$

then

$$x^2 - 2y^2 \leq u^2 - 2v^2$$

with equality if and only if $x = u$. Therefore there are infinitely many n such that

$$|u - v\sqrt{2}| < \frac{1+\epsilon}{2v\sqrt{2}}.$$

On the other hand, if

$$|u - v\sqrt{2}| < \frac{1-\epsilon}{2v\sqrt{2}}$$

then

$$\begin{aligned} |u^2 - 2v^2| &< \frac{1-\epsilon}{2v\sqrt{2}}|u - v\sqrt{2} + 2v\sqrt{2}| \\ &< \frac{1}{v} + (1-\epsilon). \end{aligned}$$

If v is sufficiently large then the last term is smaller than one and $u^2 = 2v^2$, impossible. Thus

$$a_n > \frac{1-\epsilon}{2\sqrt{2}}$$

for n sufficiently large.

8.2.6. If

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

then we have

$$x^2 \equiv -1 \mod d.$$

But then Theorem 2.5 implies that d has a primitive representation as a sum of squares.