MODEL ANSWERS TO THE FOURTH HOMEWORK

8.1.6. (a) Let

$$f(x_1+h) = f(x_1) + f'(x_0)h + \frac{1}{2}f''(x_1)h^2 + \cdots + \frac{1}{n}f^{(n)}(x_1)h^n,$$

be the Taylor expansion of $f(x)$, centred at x_1. As observed in 104A, the coefficients

$$a_i = \frac{f^{(k)}(x_1)}{k}$$

of the Taylor series expansion are all integers. By assumption

$$f(x_1) \equiv 0 \mod p^{2a+1}.$$

If $h = tp^{a+1}$ then all but the first two terms of the Taylor series expansion are divisible by p^{2a+2}. Thus we want to find t such that

$$0 = f(x_1 + tp^{a+1}) \equiv f(x_1) + f'(x_1)tp^{a+1} \mod p^{2a+2}.$$

Rearranging, gives

$$tp^{a+1}f'(x_1) \equiv -f(x_1) \mod p^{2a+1}.$$

By assumption $p^{a+1}f'(x_0)$ is divisible by p^{2a+1} but no higher power of p. As $f(x_1)$ is also divisible by p^{2a+1}, we can divide and work modulo p,

$$t \equiv \frac{-f(x_1)}{p^{a+1}f'(x_1)} \mod p.$$

With this choice of t, $x_2 = x_1 + tp^{a+1}$ satisfies

$$f(x_2) \equiv 0 \mod p^{2a+2} \qquad \text{where} \qquad x_2 \equiv x_1 \mod p^{a+1}.$$

The result then follows by an obvious induction.
(b) We want to solve the equation

$$x^2 \equiv b \mod 2^e,$$

for $e \geq 3$. Let $f(x) = x^2 - b$. Then $f'(x) = 2x$. We want to start with $e = 3$. Thus we take $a = 1$, so that $e = 2 \cdot 1 + 1 = 3$. Using part (a), if we can find x_1 odd such that

$$x_1^2 \equiv a \mod 2^3$$

then we can find solutions modulo all higher powers of 2.
If one unwraps the statement of Theorem 4.14 we get an equivalent result. We want to know that

$$a \equiv 1 \mod (2^e, 8) = 8.$$

But if x_1 is odd then $x_1^2 \equiv 1 \mod 8$.
(c) Suppose that

$$ax^2 + by^2 + cz^2 \equiv 0 \mod 8,$$

where x, y and z are all odd. Then $x^2 \equiv y^2 \equiv z^2 \equiv 1 \mod 8$. If a, b and c are all even then $a \equiv b \equiv c \equiv \pm 2 \mod 8$. This contradicts the fact that

$$ax^2 + by^2 + cz^2 \equiv 0 \mod 8.$$

Possibly rearranging, we may assume that a is odd, so that ax^2 is odd. Let

$$\alpha = -\frac{by^2 + cz^2}{a}.$$

By assumption there is a solution to the equation

$$x^2 \equiv \alpha \mod 8.$$

By part (b) we can then solve this equation modulo any power of 2 and this gives a 2-adic solution to the original equation, with the same values of y and z.
8.1.8. We are given a homogeneous quadratic equation in two variables,

$$ax^2 + bxy + cy^2 = 0.$$

If we have a solution over the integers, then we certainly have a real solution and a p-adic solution for every prime p.
Conversely suppose there is a real solution and a p-adic integer solution, for every prime p. As we have a homogeneous equation, it suffices to exhibit a rational solution, since then clearing denominators, we get an integer solution.
We first complete the square. If we multiply through by $4a$ then we get

$$(2a)^2x^2 + 4abxy + 4acy^2 = 0.$$

Replacing x by $2ax$ we may assume that $a = 1$ and b is even, so that relabelling we have

$$x^2 + 2bxy + cy^2 = 0.$$

Completing the square we get the equation

$$(x + by)^2 + (4c - b^2)y^2 = 0.$$

Subsituting for $x + by$ we are reduced to an equation of the form

$$x^2 - by^2 = 0.$$

As there a real solution we may assume that $b > 0$.
Consider the equation

$$x^2 = b.$$

By assumption if we reduce modulo p then the equation

$$x^2 = by^2 \mod p,$$

has a non-trivial solution. Thus the equation

$$z^2 \equiv b \mod p,$$

has a solution. But then Theorem 5.10 implies that b is a square and it is clear we can solve the original equation.

8.1.10. If we let

$$u = \frac{(x+1)}{y} \qquad \text{and} \qquad v = \frac{1}{x}$$

then note that

$$x = \frac{1}{v} \qquad \text{and} \qquad y = \frac{(1+v)}{u}.$$

Thus we get a birational transformation of the plane, not just a curve. Now consider how the equation

$$(x+2)y^2 = x^2(x+1)^2$$

transforms to an equation connecting u and v. Clearly we have

$$(x+2)^2 = x^2u^2.$$

Substituting for x we get

$$\left(\frac{1}{v} + 2\right)^2 = \frac{1}{v^2}u^2,$$

so that

$$(1+2v)^2 = u^2.$$

Clearly this is the equation for a conic.

8.1.11. If we substitute

$$u = \frac{x^2}{x^2+y^2} \qquad \text{and} \qquad v = \frac{xy}{x^2+y^2}$$

then we get

$$\begin{aligned} u^2 + v^2 - u &= \frac{x^4}{(x^2+y^2)^2} + \frac{x^2y^2}{(x^2+y^2)^2} - \frac{x^2}{x^2+y^2} \\ &= \frac{x^4 + x^2y^2 - x^2(x^2+y^2)}{(x^2+y^2)^2} \\ &= 0. \end{aligned}$$

Now suppose we are given u and v such that $u^2 + v^2 = u$.

8.1.12. Suppose that

$$x = \frac{t(2t^2+1)}{4t^4+1} \qquad \text{and} \qquad y = \frac{t(2t^2-1)}{4t^4+1}.$$

It is clear that if t is rational then x and y are rational.
Suppose that x and y are rational. We want to show that we can pick t rational. There are two cases. If $x \neq y$ then it is clear that t is rational from the equation

$$x^2 + y^2 = t(x - y).$$

Suppose that $x = y$. Since we have

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

It follows that $x^2 + y^2 = 0$, so that $x = y = 0$. But this corresponds to $t = 0$.
3.5.1. By definition $|0|_p = 0$. As the reciprocal of any positive real is a positive real, (ii) is clear for $|\ |$.
Suppose we are given two rational numbers a/b and c/d. Then

$$\begin{aligned}\nu_p(ac/bd) &= \nu_p(ac) - \nu_p(bd) \\ &= \nu_p(a) + \nu_p(c) - \nu_p(b) - \nu_p(d) \\ &= \nu_p(a) - \nu_p(c) + \nu_p(b) - \nu_p(d) \\ &= \nu_p(a/c) + \nu_p(b/d).\end{aligned}$$

It follows that

$$\left|\frac{ac}{bd}\right|_p = \left|\frac{a}{b}\right|_p \cdot \left|\frac{c}{d}\right|_p.$$

Suppose that we have two rational numbers q_1 and q_2. Then we may write

$$q_1 = p^e\frac{a}{b} \qquad \text{and} \qquad q_2 = p^f\frac{c}{d},$$

so that $\nu_p(q_1) = e$ and $\nu_p(q_2) = f$. But then

$$\nu_p(q_1 + q_2) \geq \min(e, f),$$

with equality unless $e = f$. It follows that

$$|q_1 + q_2|_p \leq \max(|q_1|_p, |q_2|_p),$$

with equality unless $|q_1|_p = |q_2|_p$.
3.5.2. We have to show that $a_1, a_2, \dots$ and $b_1, b_2, \dots$ generate the same equivalence class. This is equivalent to the statement that $a_1, a_2, \dots$ and $b_1, b_2, \dots$ are equivalent Cauchy sequences, that is, the difference $c_1, c_2, \dots$ is a null sequence.
Pick $\epsilon > 0$. We may find n_0 such that if m and $n > n_0$ then $|a_n - a_m| < \epsilon$. Given n, by assumption $b_n = a_m$ for some $m \geq n$. If $n > n_0$ then

$m > n_0$ and so

$$\begin{aligned}|c_n| &= |a_n - b_n| \\ &= |a_n - a_m| \\ &< \epsilon.\end{aligned}$$

It follows that $c_1, c_2, \ldots$ is indeed a null sequence.
3.5.6. (i) and (ii) are clear. (iii) does not hold. For example, if $g = 4$ then $|2|_4 = 1$ but $|4|_4 = 1/4 \neq |2|_4^2$. (iv) and (v) also hold; the proof given for primes works equally well for composite numbers.
Let $a_n = 3^{n(2^n - 2^{n-1})}$ and $b_n = 2^{n(3^n - 3^{n-1})}$. Both of these sequences are Cauchy. We have

$$|a_n|_6 = 1 \qquad \text{and} \qquad |b_n|_6 = 1,$$

so that neither $a_1, a_2, \ldots$ nor $b_1, b_2, \ldots$ are null sequences but if $c_n = a_n b_n$ then $c_n = 6^n 2^{(2^n - 2^{n-1})} 3^{(3^n - 3^{n-1})}$ so that

$$|c_n|_6 = \frac{1}{6^n},$$

and $c_1, c_2, \ldots$ is a null sequence.
3.5.7. (a) $127 = 125 + 2$ and $125 = 5^3$, so that

$$127 = 2 + 0 \cdot 5 + 0 \cdot 5^2 + 1 \cdot 5^3 + 0 \cdot 5^4 + \ldots.$$

$-2 = 3 - 5$. Now $-1 = 4 - 5$ and so

$$-2 = 3 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + \ldots.$$

Now $5/16 = 5(1/16)$, so we just have to find the reduced expansion of $1/16$. Now

$$16 = 1 + 3 \cdot 5.$$

Thus

$$\begin{aligned}\frac{1}{16} &= \frac{1}{1 + 3 \cdot 5} \\ &= 1 - 3 \cdot 5 + 9 \cdot 5^2 - 27 \cdot 5^3 + \ldots \\ &= 1 + 2 \cdot 5 + 3 \cdot 5^2 + 4 \cdot 5^3 + \ldots\end{aligned}$$

so that

$$\frac{5}{16} = 1 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + 4 \cdot 5^4 + \ldots,$$

is the reduced expansion.

$$\frac{3}{5} = \frac{1}{5}(3 + 0 \cdot 5 + 0 \cdot 5^2 + \ldots)$$

is the reduced expansion.

(b) $x^2 = 1$ has integer solutions $x = \pm 1$. These are the only solutions in $\mathbb{Q}_5$ and so

$$1 + 0 \cdot 5 + 0 \cdot 5^2 + \dots \qquad \text{and} \qquad 4 + 4 \cdot 5 + 4 \cdot 5^2 + \dots,$$

are the reduced expansions of the roots of $x^2 = 1$.
Start with the solution $x_0 = 2$ to the equation $x^2 \equiv -1 \mod 5$. Let $f(x) = x^2 + 1$. $f'(x) = 2x$ and so $f'(x_0) = 4$. On the other hand $f(x_0) = 5 = 5 \cdot 1$. Suppose that $x_1 = 2 + 5t$. Then t satisfies the equation

$$4t \equiv -1 \mod 5,$$

so that $t = 1$ and $x_1 = 2 + 1 \cdot 5$. Thus $f(x_1) = 49 + 1 = 2 \cdot 5^2$. Suppose that $x_2 = 2 + 1 \cdot 5 + t \cdot 5^2$. Then t satisfies the equation

$$4t \equiv -2 \mod 5,$$

so that $t = 2$ and $x_1 = 2 + 1 \cdot 5 + 2 \cdot 5^2$. Thus

$$\alpha = 2 + 1 \cdot 5 + 2 \cdot 5^2 + \dots$$

is one of 5-adic roots of $x^2 + 1 = 0$.
3.5.8. (a) If $p^2 | a$ then $a = p^2 b$ for some $b \in \mathbb{Z}$. If $x^2 = b$ has a solution $\beta \in \mathbb{Q}_p$ then $\alpha = p\beta \in \mathbb{Q}_p$ is a solution to the original equation $x^2 = a$. Conversely if $\alpha \in \mathbb{Q}_p$ is a solution to $x^2 = a$ then $\beta = \alpha/p$ is a solution to $x^2 = b$.
(b) If

$$\left(\frac{a}{p}\right) = 1$$

then we may find a solution x_1 to the equation $x^2 \equiv a \mod p$. As p is odd $y_1 = p - x_1$ is a different solution. It follows that we may find integers x_n and y_n that are solutions to the equation $x^2 \equiv a \mod p^n$ and such that

$$x_n \equiv x_m \mod p^{\min(m,n)} \qquad \text{and} \qquad y_n \equiv y_m \mod p^{\min(m,n)}.$$

It follows that $x_1, x_2, \dots$ and $y_1, y_2, \dots$ are Cauchy sequences so that they define elements ξ and γ of the p-adic integers $\mathcal{O}_p$. They are clearly not equal, since $x_1 \neq y_1 \mod p$. As x_n and y_n are solutions to the equation $x^2 \equiv a \mod p^n$ it follows that

$$\left|\xi^2 - a\right|_p < \frac{1}{p^n} \qquad \text{and} \qquad \left|\gamma^2 - a\right|_p < \frac{1}{p^n}$$

so that $\xi^2 = a$ and $\gamma^2 = a$ so that ξ and γ in $\mathbb{Q}_p$ are two different solutions of $x^2 = a$.
On the other hand since we have a field there are at most two solutions.

(c) If

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

then the equation $x^2 \equiv a \mod p$ has no solutions. If $\xi \in \mathbb{Q}_p$ were a solution to $x^2 = a$ then ξ would be a p-adic integer. If

$$\xi = x_0 + x_1 \cdot p + \ldots,$$

then x_0 is a solution of $x^2 \equiv a \mod p$. Thus $x^2 = a$ has no solutions in $\mathbb{Q}_p$.
Now suppose that $p|a$. If $\xi^2 = a$ and $\xi \in \mathbb{Q}$ then

$$\begin{aligned} 2\nu_p(\alpha) &= \nu_p(a) \\ &= 1, \end{aligned}$$

clearly not possible.