MODEL ANSWERS TO THE SEVENTH HOMEWORK

3.4.2. We first find the prime factorisation of 1125,

$$\begin{aligned}1125 &= 5 \cdot 225\\ &= 5^2 \cdot 45\\ &= 5^3 \cdot 9\\ &= 3^2 \cdot 5^3.\end{aligned}$$

By the Chinese remainder theorem, it suffices to find the roots modulo $9 = 3^2$ and modulo $125 = 5^3$.
We start with the problem of finding roots modulo 9. We first find the roots modulo 3. We get the equation

$$x^3 \equiv 0 \mod 3.$$

This has the single solution $x_0 = 0$. Now we use approximation to find all of the roots. $f'(x) = 3x^2$ and so $f'(x_0) \equiv 0 \mod 3$, so that x_0 is a singular solution. But $f(x_0) = 0 \mod 9$ so that every lift of 0 is a solution. Thus 0, 3 and 6 are the solutions to $x^3 - 3x^2 + 27 \equiv 0 \mod 9$.
We now consider the problem of finding the roots modulo 125. We first find the roots modulo 5. We have to solve

$$x^3 + 2x^2 + 2 \equiv 0 \mod 5.$$

By trial and error we see that $x_0 = 1$ is the only solution.
We now try to lift this to a solution modulo 25. Note that

$$f'(x) = 3x^2 - 6x$$

so that $f'(x_0) = 2 \neq 0 \mod 5$. Thus there is a unique lift. We have to solve the equation

$$5tf'(x_0) \equiv -f(x_0) \mod 25.$$

We have

$$f(x_0) = 1 - 3 + 27 = 25 \equiv 0 \mod 25.$$

As $f'(x_0) \neq 0 \mod 5$ this has the unique solution $t = 0$. Therefore $x_1 = 1$ is also a solution modulo 25. We now lift this to a solution modulo 125. We have to solve

$$25tf'(x_0) \equiv -f(x_0) \mod 125.$$

This reduces to

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

so that $t = 2$. Thus we take

$$x_2 = 1 + 2 \cdot 25 = 51.$$

Finally, to get the solution modulo 1125, we have to solve

$$\begin{aligned} x &\equiv 0 \mod 3 \\ x &\equiv 51 \mod 125. \end{aligned}$$

This gives us

$$51, \qquad 51 + 3 \cdot 125 = 426 \qquad \text{and} \qquad 51 + 6 \cdot 125 = 801.$$

3.4.3 If we apply Taylor's theorem to $f(x)$, centred at m, we get

$$\begin{aligned} f(m + kf(m)) &= f(m) + kf(m)f'(m) + k^2 f(m)^2 \frac{f''(m)}{2} + \cdots + (kf(m))^n \frac{f^{(n)}(m)}{n!} \\ &= f(m)(kf'(m) + \frac{k^2}{2} f(m)f''(m) + \cdots + \frac{k^n}{n!} f(m)^{n-1} f^{(n)}(m)). \\ &= f(m)g(k), \end{aligned}$$

where

$$g(x) = f'(m)x + \frac{x^2}{2} f(m)f''(m) + \cdots + \frac{x^n}{n!} f(m)^{n-1} f^{(n)}(m),$$

is a polynomial with rational coefficients.
First note that since the equations $f(x) = 0$, $f(x) = 1$ and $f(x) = -1$ have finitely many solutions, we may pick m so that $f(m)$ is neither zero, nor a unit (that is, ± 1). Now if we let $k = n!l$ for some integer l then $g(k)$ is an integer, since each term of the expression for $g(x)$ is an integer. As $g(x)$ is not the constant polynomial we can pick k so that $g(x)$ is neither zero, nor a unit. Thus $f(m + kf(m))$ is not prime for infinitely many integers $m + kf(m)$.
3.4.4 We first consider the case $e = 1$. We have to solve

$$x^2 \equiv a \mod 2.$$

Let $f(x) = x^2 - a$. Then $f'(x) = 2x$. If $x_0 = 0$ then $f'(x_0) = 0$ and if $x_0 = 1$ then $f'(x_0) = 2 \equiv 0$ modulo 2. Thus there every solution is singular.
3.4.5 (a) We prove this by induction on e. Let $a_1, a_2, \ldots, a_s$ be the s distinct non-singular solutions modulo p. Let $b_1, b_2, \ldots, b_s$ be their lift to solutions modulo p^e. We have

$$f'(b_i) \equiv f'(a_i) \neq 0 \mod p.$$

Thus b_i is a non-singular solution. Thus we may lift b_i to a solution c_i modulo p^{e+1}.

(b) We already know that $x^d - 1 = 0$ has d solutions modulo p. Let $f(x) = x^d - 1$. Then $f'(x) = dx^{d-1}$. If a_i is a solution to

$$x^d - 1 \equiv 0 \mod p,$$

then $a_i \neq 0$ so that $f'(a_i) \neq 0 \mod p$. By (a) we may lift each of the d solutions to d distinct solutions modulo p^e, for every e. On the other hand, every solution modulo p^e is a solution modulo p, so that there are at most d solutions modulo p^e. Thus there are exactly d solutions.
3.4.7 We prove this by induction on k. If $k = 1$ then this is Wilson's theorem. Suppose we know the result for $k < p - 2$. Note that

$$\begin{aligned}(p-k-1)!k! &= k(p-k-1)!(k-1)! \\ &\equiv -(p-k)(p-k-1)!(k-1)! \mod p \\ &= -(p-k)!(k-1)! \\ &\equiv -(-1)^k \mod p \\ &= (-1)^{k+1}.\end{aligned}$$

Thus we are done by induction on k.
3.4.8 Suppose that

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

Then

$$\begin{aligned}f(a_0 x) &= a_0 + a_1(a_0 x) + a_2(a_0 x)^2 + \cdots + a_n(a_0 x)^n \\ &= a_0(1 + a_1 x + a_2 a_0 x^2 + \cdots + a_n a_0^{n-1} x^n) \\ &= a_0(1 + x(a_1 + a_2 a_0 x + \cdots + a_n a_0^{n-1} x^{n-1}) \\ &= a_0(1 + xg(x)),\end{aligned}$$

where $g(x)$ is a polynomial of degree $n-1$. Note that $g(x) \neq 0$ as $f(x)$ is not constant. Suppose that $p_1, p_2, \dots, p_k$ is a sequence of finitely many primes. Let m be the product and let l be a natural number. Then

$$1 + lmg(lm) \equiv 1 \mod m.$$

It follows that $f(a_0 lm)$ is not divisible by any of the primes $p_1, p_2, \dots, p_k$. $g(x)$ has only finitely many zeroes, so we may choose l so that $g(lm) \neq 0$. By the fundamental theorem of arithmetic, it follows that $f(a_0 lm)$ is divisible by a prime p, not belonging to the sequence $p_1, p_2, \dots, p_k$. In this case $f(x) \equiv 0 \mod p$.
3.4.10 Not quite; if $p = 2$ then $-1 = 1 = 1^2$ is a square.
Let's assume that p is an odd prime. By Euler's criterion,

$$\left(\frac{-1}{p}\right) = 1 \qquad \text{if and only if} \qquad (-1)^{(p-1)/2} \equiv 1 \mod p.$$

If $p \equiv 1 \mod 4$ then there is an integer k such that $p = 4k+1$. In this case

$$\frac{p-1}{2} = 2k,$$

so that

$$(-1)^{(p-1)/2} = 1.$$

Therefore -1 is a square modulo p if $p \equiv 1 \mod 4$.
If p is odd then the only other possibility is that $p \equiv 3 \mod 4$. In this case there is an integer k such that $p = 4k+3$. It follows that

$$\frac{p-1}{2} = 2k+1,$$

so that

$$(-1)^{(p-1)/2} = -1.$$

Thus -1 is not a square modulo p if $p \equiv 3 \mod 4$.
3.4.11 We want to prove that if

$$(m-1)! \equiv -1 \mod m,$$

then m is a prime.
Suppose that m is composite. Then we may write $m = ab$, where $a > 1$ and $b > 1$. First suppose that we can choose a and b such that $a < b$. Then

$$\begin{aligned}(m-1)! &= (m-1)(m-2)\dots(b+1)b\cdot(b-1)\dots(a+1)\cdot a\cdot(a-1)\dots\\ &= abk\\ &= 0 \mod m,\end{aligned}$$

where k is an integer.
If m is composite and we cannot choose $a \neq b$ then $m = p^2$ is the square of a prime. Suppose that $p > 2$. Then

$$\begin{aligned}(m-1)! &= (p^2-1)(p^2-2)\dots(2p+1)(2p)(2p-1)\dots(p+1)p(p-1)\dots\\ &= p^2k\\ &= 0 \mod m,\end{aligned}$$

where k is an integer. The remaining case is $m = 4 = 2^2$. In this case

$$\begin{aligned}(m-1)! &= 3!\\ &= 6\\ &\neq -1 \mod m = 4.\end{aligned}$$

Thus if

$$(m-1)! \equiv -1 \mod m,$$

then m is a prime.