1. Find all solutions to the congruence

$$x^4 + 6x^3 + 302x^2 + 6x + 301 \equiv 0 \pmod{343}.$$

Solution: Let $f(x) = x^4 + 6x^3 + 302x^2 + 6x + 301$. Working first modulo 7, the congruence reads

$$x^4 + 6x^3 + x^2 + 6x \equiv 0 \pmod{7}.$$

We factor this to get $x(x+6)(x^2+1)$, so the solutions to $f(x) \equiv 0 \pmod{7}$ are $x = 0$ and $x = 1$. The factor $x^2 + 1$ has no roots modulo 7, because $7 \equiv 3 \pmod{4}$.

We next need $f'(x)$, but since we only need a representative of $f'(x)$ modulo 7, we can take

$$\begin{aligned} f'(x) &\equiv 4x^3 + 18x^2 + 2x + 6 \pmod{7} \\ &\equiv 4x^3 + 4x^2 + 2x + 6 \pmod{7}. \end{aligned}$$

We then easily find that $f'(0) \equiv 6 \pmod{7}$ and $f'(1) \equiv 2 \pmod{7}$. The multiplicative inverses of these numbers (found more or less by trial and error) are

$$\overline{f'(0)} \equiv 6 \pmod{7} \qquad \overline{f'(1)} \equiv 4 \pmod{7}.$$

We now lift the root 0 modulo 7 to a root modulo 49. Since $f(0) = 301 \equiv 7 \pmod{49}$, we get

$$0 - 6 \times 7 \equiv -42 \equiv 7 \pmod{49}$$

so one root of $f(x) \equiv 0 \pmod{49}$ is 7.

We lift the root 1 modulo 7 to a root modulo 49 in the same way: First, we have $f(1) = 616 \equiv 28 \pmod{49}$. The corresponding solution to $f(x) \equiv 0 \pmod{49}$ is

$$1 - 28 \times 4 \equiv -111 \equiv 36 \pmod{49}.$$

We now lift the roots 7 and 36 modulo 49 to solutions to $f(x) \equiv 0 \pmod{343}$. We first observe that $f(7) \equiv 49 \pmod{343}$, so the root 7 lifts to

$$7 - f(7) \times 6 = 7 - 49 \times 6 \equiv 7 + 49 \equiv 56 \pmod{343}.$$

For 36, we observe that $f(36) \equiv 196 \pmod{343}$ so this root lifts to

$$36 - f(36) \times 4 \equiv 36 + 3 \times 196 \equiv 281 \pmod{343}.$$

There are two solutions to the original congruence:

$$\begin{aligned} x &\equiv 56 \pmod{343} \text{ and} \\ x &\equiv 281 \pmod{343}. \end{aligned}$$

2. Let $f(x) = x^3 + 27x^2 + 80x + 49$. Solve each of the congruences

$$f(x) \equiv 0 \pmod{5}, \quad f(x) \equiv 0 \pmod{25}, \quad \text{and} \quad f(x) \equiv 0 \pmod{125}.$$

How many solutions are there to the congruence $f(x) \equiv 0 \pmod{625}$?

Solution: We begin working modulo 5, where our congruence reads

$$x^3 + 2x^2 + 4 \equiv 0 \pmod{5}.$$

By simply trying each of the value 0, 1, 2, 3, and 4, for x, we find that the solutions of this congruence are $x = 2$ and $x = 4$.

Still working modulo 5, we find that $f'(x) \equiv 3x^2 + 4x$, so that $f'(2) \equiv 12 + 8 \equiv 0 \pmod{5}$ and $f'(4) \equiv 3 + 1 \equiv 4 \pmod{5}$.

This means the root 4 will lift to a unique root modulo 5^j for each $j > 1$, and the root 2 may lift to zero or five roots each time we increase the power of 5 in the modulus.

Lifting 4 first, we find that $\overline{f'(4)} = 4$ and

$$f(4) = 865 \equiv 15 \pmod{25}$$

so that one root of $f(x) \equiv 0 \pmod{25}$ is

$$4 - 15 \times 4 = -56 \equiv 19 \pmod{25}.$$

For the singular root 2, we find that

$$f(2) = 325 \equiv 0 \pmod{25}$$

so that 2, 7, 12, 17, and 22 are all roots of $f(x) \equiv 0 \pmod{25}$. The complete list of roots modulo 25 is

$$2,\ 7,\ 12,\ 17,\ 19,\ 22.$$

On to modulus 125. The non-singular root 19 of $f(x) \equiv 0 \pmod{25}$ will lift to a unique root of $f(x) \equiv 0 \pmod{125}$. Since $f(19) \equiv 50 \pmod{125}$, the lift of the root 19 is

$$19 - f(19) \times 4 \equiv 19 + f(19) \equiv 219 \equiv 69 \pmod{125}.$$

Each of the remaining roots r modulo 25 will lift to zero or five roots modulo 125 according to whether $f(r) \equiv 0 \pmod{125}$. Using a computer to do the grunt-work, we find that

$$\begin{aligned} f(2) &\equiv 75 \pmod{125} \\ f(7) &\equiv 25 \pmod{125} \\ f(12) &\equiv 0 \pmod{125} \\ f(17) &\equiv 0 \pmod{125} \\ f(22) &\equiv 25 \pmod{125} \end{aligned}$$

The root 12 lifts to five roots $12 + 25k$, with $k = 0, 1, \ldots, 4$; the root 17 similarly lifts to $17 + 25k$. The complete list of roots to $f(x) \equiv 0 \pmod{125}$ is

$$12,\ 17,\ 37,\ 42,\ 62,\ 67,\ 69,\ 87,\ 92,\ 112,\ 117.$$

The singular root 69 will lift to a unique root modulo 625. For each of the other roots r, we check whether $f(r) \equiv 0 \pmod{625}$. Again using a computer, we find that only $f(37)$ and $f(117)$ are divisible by 625. Each of these lifts to five roots, so the number of solutions to $f(x) \equiv 0 \pmod{625}$ is eleven.

3. (§27, problem 6) Theorem 2.26 states that if p is prime and $f(x)$ is a polynomial with integer coefficients then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n solutions, where n is the degree of the congruence.

Show that the hypothesis that p is prime is necessary. That is, for some composite number m, find an example of a congruence $f(x) \equiv 0 \pmod{m}$ with degree n and more than n roots.

Solution: The congruence in the previous problem will do (read either modulo 125 or modulo 625), since it has degree 3 and rather more than three roots.

4. Let $f(x)$ be a polynomial with integer coefficients, and let p be a prime. Suppose x_1 and x_2 are integers such that $x_1 \not\equiv x_2 \pmod{p^2}$, $f(x_1) \equiv f(x_2) \pmod{p^2}$, and $x_1 \equiv x_2 \pmod{p}$. Prove that

$$f'(x_1) \equiv f'(x_2) \equiv 0 \pmod{p}.$$

Proof: Let n be the degree of f. By Taylor's theorem,

$$\begin{aligned} f(x_2) &= f(x_1) + (x_2 - x_1)f'(x_1) + \frac{(x_2 - x_1)^2 f''(x_1)}{2!} + \cdots + \frac{(x_2 - x_1)^n f^{(n)}(x_1)}{n!} \\ &\equiv f(x_1) + (x_2 - x_1)f'(x_1) \pmod{p^2} \end{aligned}$$

because $(x_2 - x_1)^k$ is divisible by p^2 for each $k > 1$, and $f^{(k)}(x_1)/k!$ is an integer for each k. This gives us

$$\begin{aligned} (x_2 - x_1)f'(x_1) &\equiv f(x_2) - f(x_1) \pmod{p^2} \\ &\equiv 0 \pmod{p^2}, \end{aligned}$$

so that p^2 divides $(x_2 - x_1)f'(x_1)$. Now we know $p|(x_2 - x_1)$, but $p^2 \not| (x_2 - x_1)$, so we can write $(x_2 - x_1) = pm$ where m is an integer not divisble by p. Then we have

$$p^2 | pmf'(x_1), \text{ from which we get } p|mf'(x_1),$$

and since p is prime and $p \not| m$, we conclude that $p|f'(x_1)$. Thus $f'(x_1) \equiv 0 \pmod{p}$. Now since $x_1 \equiv x_2 \pmod{p}$ and f' is a polynomial with integer coefficients, Theorem 2.2 tells us that $f'(x_1) \equiv f'(x_2) \pmod{p}$, so $f'(x_2) \equiv 0 \pmod{p}$ as well. ∎

5. (a) Consider the sequence $\{s_n\}$ given by

$$s_k = 3 + 2 \times 5 + 2 \times 5^2 + 2 \times 5^3 + \cdots + 2 \times 5^k.$$

Prove by that $2s_k - 1 = 5^{k+1}$ for each integer $k \geq 0$. Use this result to prove that the 5-adic number $3 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + \cdots$ is equal to $\frac{1}{2}$.

Solution: Proof: We recall that for any real number $x \neq 1$ and each non-negative integer k,

$$1 + x + x^2 + \cdots + x^k = \frac{(x^{k+1} - 1}{x - 1).}$$

We can use this to simplify our expression for s_k. We get

$$\begin{aligned} s_k &= 1 + 2(1 + 5 + 5^2 + \cdots + 5^k) \\ &= 1 + 2\left(\frac{5^{k+1} - 1}{5 - 1}\right) \\ &= 1 + \frac{5^{k+1} - 1}{2}. \end{aligned}$$

Thus we have

$$2s_k - 1 \;=\; 5^{k+1}$$

for each integer $k \geq 0$.

From this, we may deduce that

$$\begin{aligned} \left| s_k - \frac{1}{2} \right|_5 &= \left| \frac{2s_k - 1}{2} \right|_5 \\ &= \left| \frac{5^{k+1}}{2} \right|_5 \\ &= \frac{1}{5^{k+1}}, \end{aligned}$$

so that

$$\lim_{k \to \infty} \left| s_k - \frac{1}{2} \right|_5 \;=\; 0.$$

That is, the Cauchy sequence $\{s_k\}$ (also represented by the 5-adic number $3 + 2 \cdot 5 + 2 \cdot 5^2 + \ldots$) is equivalent to the sequence $\{1/2, 1/2, 1/2, \ldots\}$, which represents the rational number $\dfrac{1}{2}$.

(b) Find 5-adic representations of the form $5^N(d_0 + d_1 \cdot 5 + d_2 \cdot 5^2 + d_3 \cdot 5^3 + \cdots)$ (with each d_i a non-negative integer) for the numbers -2 and $\dfrac{1}{3}$.

Solution: Let $f(x) = x+2$. We want to solve the congruence $f(x) \equiv 0 \pmod{5^k}$ for $k = 1, 2, 3, \ldots$. The solution with $k = 1$ is clearly 3.

To lift 3 to a solution modulo 25, we compute

$$\begin{aligned} f(3) &= 5 \\ f'(3) &= 1 \end{aligned}$$

and solve

$$f'(3) \equiv -\frac{f(3)}{5} \pmod{5}$$

We get $t = 4$, so our mod-25 solution is $3 + 4 \cdot 5 = 23$.

To lift this solution to a solution modulo 125, we compute

$$f(23) = 25$$
$$f'(23) = 1$$

and solve

$$f'(3) = -\frac{f(23)}{25} \pmod 5.$$

We get $t = 4$ again, so our mod-125 solution is $3 + 4 \cdot 5 + 4 \cdot 25 = 123$.

We suspect that the pattern continues, and conjecture that

$$-2 = 3 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + \cdots$$

in the 5-adic field. To verify this conjecture, we set

$$s_k = 3 + 4 \cdot 5 + \cdots + 4 \cdot 5^k$$

and note that

$$\begin{aligned} s_k + 2 &= 5 + 4(5 + 5^2 + 5^3 + \cdots 5^k) \\ &= 1 + 4\left(\frac{5^{k+1} - 1}{4}\right) \\ &= 4 \cdot 5^{k+1} \end{aligned}$$

so that $|s_k + 2|_5 = \dfrac{1}{5^{k+1}}$. Thus

$$\lim_{k \to \infty} |s_k + 2|_5 = 0$$

so the sequence $\{s_k\}$ is equal to -2 as a 5-adic number.

Applying the usual techniques to solve the congruence $3x - 1 \equiv 0 \pmod{5^k}$ for increasing values of k, we find, for example, that

$$x = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4$$

is a solution modulo 5^5. We suspect that the pattern 1, 3, 1, 3, continues, and conjecture that the number we seek is

$$x_0 = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + \cdots$$

To verify this conjecture, we let

$$\begin{aligned} s_k &= 2 + 8 \cdot 5 + 8 \cdot 5^3 + 8 \cdot 5^5 + \cdots + 8 \cdot 5^{2k+1} \\ &= 2 + 5(8 + 8 \cdot 5^2 + 8 \cdot 5^4 + \cdots + 8 \cdot 5^{2k}) \\ &= 2 + 40 \left(\frac{25^{k+1} - 1}{25 - 1} \right) \end{aligned}$$

Then the sequence $\{s_k\}$ converges to our number x_0. Furthermore, we have

$$\begin{aligned} 3s_k - 1 &= 6 + 120 \left(\frac{25^{k+1} - 1}{24} \right) - 1 \\ &= 5 + 5(25^{k+1} - 1) \\ &= 5 \cdot 25^{k+1} \\ &= 5^{2k+3}. \end{aligned}$$

Thus $|3s_k - 1|_5 = \dfrac{1}{5^{2k+3}}$. Since $\left|\dfrac{1}{3}\right|_5 = 1$, we get

$$\left| s_k - \frac{1}{3} \right|_5 = \left|\frac{1}{3}\right|_5 \cdot |3s_k - 1|_5 = \frac{1}{5^{2k+3}},$$

which goes to 0 as $k \to \infty$. Thus the sequence $\{s_k\}$ converges to $\dfrac{1}{3}$ as a 5-adic number.