Problem 4 sec 2.6. Solve $x^2 + 5x + 24 \equiv 0 \pmod{36}$.

**Solution.** It is important to realize that, even though $36 = 6^2$, you cannot solve this mod 6 and then lift roots because the lifting roots method only works for prime powers.

To deal with this, we recall that $f(x) \equiv 0 \pmod{mn}$ is equivalent to a system of two congruences, $f(x) \equiv 0 \pmod{m}$ and $f(x) \equiv 0 \pmod{n}$ whenever $(m, n) = 1$. So we need to find simultaneous solutions of $x^2 + 5x + 24 \equiv 0 \pmod{4}$ and $x^2 + 5x + 24 \equiv 0 \pmod{9}$. Now $9 = 3^2$ and $4 = 2^2$, so one can in principle find roots mod 2 and mod 3 and lift them, but it’s quicker to just do a case-by-case analysis of residues mod 9 and mod 4. We find that $x \equiv 6$ or $x \equiv 7 \pmod{9}$, and $x \equiv 0$ or $x \equiv 3 \pmod{4}$. Now, since $(4, 9) = 1$, $x \equiv 6 \pmod{9}$ gives the following possibilities mod 36: $6$, $6 + 9 = 15$, $6 + 2 \cdot 9 = 24$, $6 + 3 \cdot 9 = 33$, and $7$, $7 + 9 = 16$, $7 + 2 \cdot 9 = 25$, $7 + 3 \cdot 9 = 34$. Checking this against the mod 4 restrictions, we get solutions $x \equiv 7$, $15$, $16$, $24 \pmod{36}$.

Problem 3 sec 2.6. Solve $x^3 + x^2 - 5 \equiv 0 \pmod{7^3}$.

**Solution.** Use the method described in sec 2.6. First find roots mod 7, by checking residues mod 7 and seeing that only $x \equiv 2 \pmod{7}$ works. Next, if $x \equiv a$ is a root mod 7, we look for a root mod $7^2$ of the form $a + 7t$, where, as long as $f'(a) \neq 0$, $t$ can be found as the unique solution of

$$ tf'(a) \equiv -\frac{f(a)}{7} \pmod{7}; $$

here $f(x) = x^3 + x^2 - 5$. Plug in $f(2) = 7$ and $f'(2) = 16$, solve $16t \equiv -1 \pmod{7}$, i.e $2t \equiv -1 \pmod{7}$, to find $t \equiv 3$ and $x \equiv 23$ the unique solution of $x^3 + x^2 - 5 \equiv 0 \pmod{7^2}$. Then use the same procedure once again, to find a root mod $7^3$ of the form $23 + 7t^2$. The answer will be $t \equiv 0$ and so $x \equiv 23$ the unique solution of $x^3 + x^2 - 5 \equiv 0 \pmod{7^3}$.

Problem 3 sec 2.7. Prove that $x^{14} + 12x^2 \equiv 0 \pmod{13}$ is an identical congruence.

**Solution.** Write $x^{14} + 12x^2 = x(x^{13} - x) + 13x^2 \equiv x(x^{13} - x)$ and use Fermat’s theorem.


**Solution.** As $\phi(23) = 22 = 2 \cdot 11$, the order of a number mod 23 can only be 2, 11, or 22. We want it to be 22, i.e we’re looking for $a$ such that $a^{22} \equiv 1 \pmod{23}$ but $a^{11}$ and $a^2$ are not congruent to 1. People who solved this question found (after some painful multiplication) that $a = 5$ works. You can, however, reduce the amount of calculation recalling that if $a$ has order 2, and $b$ has order 11, then $ab$ has order 22. It remains to find residues of order 2 and of order 11. Order 2 means it’s a solution of $x^2 \equiv 1$, so $x \equiv \pm 1$ and so $-1$ is the only element of order 2. To find an element of order 11, notice that since $(x^{11})^2 \equiv 1$, we can only have $x^{11} \equiv -1$ (then $x$ is a primitive root) or $x^{11} \equiv 1$ (then it is not). But consider, for example, $2^{11}$ and $(-2)^{11}$. One of them will equal to $+1$, the other
to $-1$. So if we compute $2^{11} \mod 23$, we’ll know which of the two possibilities is the case, and will determine whether $2$ or $-2$ gives a primitive root. We can even avoid calculations altogether, since $(-4)^{11} = 2^{11} \cdot (-2)^{11} \equiv (+1) \cdot (-1) \equiv -1 \mod 23$, so $-4$ is a primitive root.

**Problem 9 sec 2.8.** Check that $3^8 \equiv -1 \mod 17$, explain why this implies that 3 is a primitive root mod 17.

**Solution.** $3^8 \equiv -1 \mod 17$ is a calculation. Since $\phi(17) = 16$, the order of 3 mod 17 is a divisor of 16. If it were not 16, it would be divisor of 8, then we’d have $3^8 \equiv +1 \mod 17$. 