

We first try to solve a simple case of congruent equations:

$$\begin{aligned} p(x) &\equiv 1 \pmod{(x+1)^2}, \\ p(x) &\equiv 0 \pmod{(x+2)^3}. \end{aligned}$$

Solutions really exist: since $(x+1)^2$ and $(x+2)^3$ are coprime (relatively prime), we can find polynomials $a(x)$ and $b(x)$ such that $a(x)(x+1)^2 + b(x)(x+2)^3 = 1$. The polynomial $\beta(x) := b(x)(x+2)^3$ is just a solution. Similarly, we can also solve the following equations:

$$\begin{aligned} p(x) &\equiv 0 \pmod{(x+1)^2}, \\ p(x) &\equiv 1 \pmod{(x+2)^3}. \end{aligned}$$

Actually, $\alpha(x) := a(x)(x+1)^2$ is just a solution to this equations. Thus the combination $2x\beta(x) + 3x\alpha(x)$ solves the original congruent equations (properties in the above remark).

Now we are left to show how to find $a(x)$ and $b(x)$, but the procedure is already given in the lecture notes: let us apply the Euclidean algorithm to $(x+2)^3$ and $(x+1)^2$. We have

$$\begin{aligned} (x-2)^3 &= (x-1)^2(x-4) + (3x-4). \\ (x-1)^2 &= (3x-4)\left(\frac{1}{3}x - \frac{2}{9}\right) + \frac{1}{9} \text{ or simply, } 9(x-1)^2 = (3x-4)(3x-2) + 1. \end{aligned}$$

Thus,

$$\begin{aligned} 1 &= 9(x-1)^2 - (3x-4)(3x-2) \\ &= 9(x-1)^2 - ((x-2)^3 - (x-1)^2(x-4))(3x-2) \\ &= (x-1)^2(3x^2 - 14x + 17) - (x-2)^3(x-2). \end{aligned}$$

Substituting $(3x^2 - 14x + 17)$ and $-(x-2)^3$ for $a(x)$ and $b(x)$, we conclude that $p(x) = 3x^5 - 20x^4 + 48x^3 - 48x^2 + 19x - 12$ is one solution to the original equations. In order to find the solution with the smallest degree, we consider the following claim: suppose $q(x)$ is an arbitrary polynomial, it solves this problem if and only if $q(x) \equiv p(x) \pmod{(x-1)^2(x-2)^3}$ (Why?). After knowing this, we try to divide $p(x)$ by $(x-1)^2(x-2)^3$ and obtain

$$p(x) = 3(x+1)^2(x+2)^3 + 4x^4 - 27x^3 + 66x^2 - 65x + 24.$$

This reminder $4x^4 - 27x^3 + 66x^2 - 65x + 24$ is the required result as we cannot lower the degree any more. The total process of solving this problem is known as the celebrated **Chinese remainder theorem** (a formal proof is given in the following for people familiar with the language of rings and ideals).

As an additional exercise, can you use a similar argument to solve the following equations:

$$\begin{aligned} x &\equiv -1 \pmod{15} \\ x &\equiv 3 \pmod{11} \end{aligned}$$

What about

$$\begin{aligned} x &\equiv -1 \pmod{15} \\ x &\equiv 3 \pmod{11} \\ x &\equiv 6 \pmod{8} \end{aligned}$$