

Math 55 — Discrete Mathematics — Spring 2003

Quiz 3 Solutions

Use the Chinese remainder theorem to find all solutions of the congruence

$$x^2 \equiv 4 \pmod{35}$$

or, on the other version of the quiz,

$$x^2 \equiv 9 \pmod{35}.$$

First we find the solutions $\pmod{5}$ and $\pmod{7}$. For the first version, the four possibilities are

$$\begin{aligned}x &\equiv 2 \pmod{5}; & x &\equiv 2 \pmod{7}, \\x &\equiv 2 \pmod{5}; & x &\equiv -2 \pmod{7}, \\x &\equiv -2 \pmod{5}; & x &\equiv 2 \pmod{7}, \\x &\equiv -2 \pmod{5}; & x &\equiv -2 \pmod{7}.\end{aligned}$$

For the second version, they are

$$\begin{aligned}x &\equiv 3 \pmod{5}; & x &\equiv 3 \pmod{7}, \\x &\equiv 3 \pmod{5}; & x &\equiv -3 \pmod{7}, \\x &\equiv -3 \pmod{5}; & x &\equiv 3 \pmod{7}, \\x &\equiv -3 \pmod{5}; & x &\equiv -3 \pmod{7}.\end{aligned}$$

One reason why there are no solutions other than the obvious ones $x \equiv \pm 2 \pmod{5}$ and $\pmod{7}$, or $x \equiv \pm 3$ for version two, is that 5 and 7 are prime. You could also verify this by checking all possible remainders. Next we recover the solutions $\pmod{35}$ by using the Chinese remainder theorem. The basic solutions are the same for both versions:

$$\begin{aligned}x_1 &\equiv 1 \pmod{5}, & x_1 &\equiv 0 \pmod{7} &\Rightarrow & x_1 &\equiv 21 \pmod{35} \\x_2 &\equiv 0 \pmod{5}, & x_2 &\equiv 1 \pmod{7} &\Rightarrow & x_2 &\equiv 15 \pmod{35}.\end{aligned}$$

The four solutions for the first version are now

$$\begin{aligned}x &\equiv 2 \cdot 21 + 2 \cdot 15 \equiv 2 \pmod{35}, \\x &\equiv 2 \cdot 21 - 2 \cdot 15 \equiv 12 \pmod{35}, \\x &\equiv -2 \cdot 21 + 2 \cdot 15 \equiv -12 \pmod{35}, \\x &\equiv -2 \cdot 21 - 2 \cdot 15 \equiv -2 \pmod{35},\end{aligned}$$

and for the second,

$$\begin{aligned}x &\equiv 3 \cdot 21 + 3 \cdot 15 \equiv 3 \pmod{35}, \\x &\equiv 3 \cdot 21 - 3 \cdot 15 \equiv 18 \pmod{35}, \\x &\equiv -3 \cdot 21 + 3 \cdot 15 \equiv -18 \pmod{35}, \\x &\equiv -3 \cdot 21 - 3 \cdot 15 \equiv -3 \pmod{35}.\end{aligned}$$