

7.14 4a: By the proof of 7.13, we have that

$$16^2 = 6 + 5^3 \cdot 2$$

We have that $q = 2, r = 16, p = 5, i = 3$ with k unknown. So therefore we have that $s = 16 + 5^4 k$ and so $s^2 = r^2 + 2rp^i k + p^{2i} k^2 \equiv a + (q + 2 + rk)p^i \pmod{p^{i+1}}$. So we want to solve the following:

$$q + 2rk \equiv 0 \pmod{5} \implies 2 + 2(16)k \equiv 0 \pmod{5}$$

And we see that $k = 4$ solves. Therefore $s = 16 + 5^3 \cdot 4 = 516$. Thus the square roots of $6 \pmod{54}$ are ± 516 .

7.16a: We see that $41 \equiv 3^2 \pmod{2^5}$ with $r = 3$ and so $3^2 = 41 + 2^5 \cdot -1$. We see that $q = -1$ when $k = 1$. Therefore $q + rk = -1 + 3 \cdot 1 = 2$. Thus $s = 13 + 2^4 \cdot 1 = 19$ is a square root of $41 \pmod{2^6}$. Multiplying by ± 1 and ± 31 we get that ± 19 and ± 13 are our desired square roots.

7.18: We know that $168 = 3 \cdot 7 \cdot 8$. By the previous results we will work with $25 \equiv 1 \pmod{2^3}, 25 \equiv 1 \pmod{3}, 25 \equiv 4 \pmod{7}$. These will have solutions of $s \equiv 1 \pmod{2}, s \equiv \pm 1 \pmod{3}, s \equiv \pm 2 \pmod{7}$. By CRT, the solutions are $s \equiv \pm(5, 19, 23, 37, 47, 61, 65, 79) \pmod{168}$.

7.26: We have that $513 = 3^3 \cdot 19$. Hence the square roots of $7 \pmod{3^3}$ is $s = \pm 13 \pmod{3^3}$ and $7 \pmod{19}$ will have square root of $s = \pm 8 \pmod{19}$. By CRT the square root will be $s = \pm 68, 122 \pmod{51368}$.