

Q2a: We want to compute $[5^{4100}]_{36}$. We first set $m = \lfloor \log_2(4100) \rfloor = 12$. Next, we compute $[r_i] = [5^{2^i}]_{36}$ for i from 1 to m . When i is odd, we see that $[r_i]_{36} = 25$ and for even i , $[r_i]_{36} = 13$. Next, we represent 4100 as a binary number, $4100 = 2^{12} + 2^2$. Finally, the last step in our algorithm is to solve $[5^{4100}]_{36} = [r_{12}]_{36} \cdot [r_2]_{36} = [25]_{36}$

Q2b: We want to compute $[2^{32790}]_{77}$. We first set $m = \lfloor \log_2(32790) \rfloor = 15$. Next we compute $[r_i] = [2^{2^i}]_{77}$ for i from 1 to m . We see that $[r_1]_{77} = 4$, $[r_2]_{77} = 16$, $[r_3]_{77} = 25$ and $[r_4]_{77} = 9$. This pattern will repeat as we increase i . We now write $32790 = 2^{15} + 2^4 + 2^2 + 2^1$, and by our algorithm we have that $[2^{32790}]_{77} = [r_{15} \cdot r_4 \cdot r_2 \cdot r_1]_{77} = [1]_{77}$.

Q2c: We can set $m = \lfloor \log_2(50) \rfloor = 5$. Then we compute $[(x+1)^{2^i}]_{x^3+x^2+1}$ for i ranging from 1 to m . We see that $(x+1)^2 \equiv x^2 + 1$, $(x+1)^{2^2} \equiv x^2 + x$ and $(x+1)^{2^3} \equiv x + 1$ with the pattern repeating. In binary expansion, we have that $50 = 2^5 + 2^4 + 2^1$ and so we compute $(x+1)^{50} \equiv (x^2 + 2)(x^2 + 1)(x^2 + 1) \equiv x \pmod{x^3 + x^2 + 1}$

Q2d: Set $m = \lfloor \log_2(200) \rfloor = 7$. Then we compute $[x^{2^i}]_{x^3+x+1}$ for i ranging from 1 to m . We see $[x^{2^1}]_{x^3+x+1} = x^2$, $[x^{2^2}]_{x^3+x+1} = -x^2 - x$, $[x^{2^3}]_{x^3+x+1} = 2x + 3$, $[x^{2^4}]_{x^3+x+1} = -x^2 + 2x - 1$, $[x^{2^5}]_{x^3+x+1} = -x$, repeating every 5 i . We know that 200 has a binary expansion of $200 = 2^7 + 2^6 + 2^3$. Therefore, by our algorithm,

$$[x^{200}]_{x^3+x+1} \equiv (-x - x^2)(x^2)(2x + 3) \equiv 2x^2 + x + 1 \pmod{x^3 + x + 1}$$