Solutions to Assignment 9

I1a*. Find an integer X such that $X^2 \equiv 5 \bmod 31$ follows.
How do we also know $X^{32} \equiv 5 \bmod 31$?

It is easy to see that if X = 6, $X^2 = 36 \equiv 5 \bmod 31$.

Note that $X^{32} = X^{30} \bullet X^2$ and by Fermat's Little Theorem, $X^{30} \equiv 1 \bmod 31$ (6 and 31 are relatively prime to each other).

So, $X^{32} = X^{30} \bullet X^2 \equiv 1 \bullet X^2 = X^2 = 36 \equiv 5 \bmod 31$.

b*. $X^{32} \equiv ((X^2)^8)^2 \equiv (5^8)^2$ 5 mod 31.

Compute (the smallest nonnegative) $X \equiv 5^8 \bmod 31$.

Check $5 \equiv X^2 \bmod 31$.

$X \equiv 5^8 \bmod 31$. Let's reduce $5^8 \bmod 31$:

$5^8 = 5^3 \bullet 5^3 \bullet 5^2$. But, $5^3 = 125 = 31 \bullet 4 + 1$.

$\Rightarrow 5^3 \equiv 1 \bmod 31$.

So, $5^8 = 5^3 \bullet 5^3 \bullet 5^2 \equiv 1 \bullet 1 \bullet 5^2 = 5^2 \bmod 31$.

Thus, $5^8 \equiv 25 \bmod 31 \Rightarrow X = 25$.

Check $5 \equiv X^2 \bmod 31$:

$X^2 = 25^2 = 5^3 \bullet 5 \equiv 1 \bullet 5 \equiv 5 \bmod (31)$.

I2. Compute $Y \equiv 10^{11} \bmod 43$.

Explain why Y is a squareroot of 10 mod 43.

$10^{11} = 10^5 \bullet 10^5 \bullet 10^1$. Using a calculator, it is easily seen that $10^5 \equiv 25 \bmod 43$.

So, $10^5 \bullet 10^5 \equiv 25 \bullet 25 = 625 \equiv 23 \bmod 43$.

So, $10^5 \bullet 10^5 \bullet 10^1 \equiv 23 \bullet 10 = 230 \equiv 15 \bmod 43$.

Thus, Y = 15.

To show Y is a squareroot of 10 mod 43, we need to show that $Y^2 \equiv 10 \bmod 43$.

$Y^2 = 15^2 = 225 = 43 \bullet 5 + 10$.

So, $225 \equiv 10 \bmod 43$.

Thus, $Y^2 \equiv 10 \bmod 43 \Rightarrow Y$ is a squareroot of 10 mod 43.