

Homework 20

Find 8 different solutions to $x^2 \equiv 1 \pmod{9775}$.

(Note, $n = 9775$ factors as $5^2 \cdot 17 \cdot 23$. If we were using the Rabin-Miller test on 9775 , then the general theory tells us that there should be 2^3 solutions to this congruence because there are 3 primes dividing n and n is odd.)

Homework 20 Solution

First, we factor $9775 = 5^2 \cdot 17 \cdot 23$ and note that by the CRT, $x^2 \equiv 1 \pmod{9775}$ is equivalent to the system of congruences

$$x^2 \equiv 1 \pmod{5^2}$$

$$x^2 \equiv 1 \pmod{17}$$

$$x^2 \equiv 1 \pmod{23}$$

Each of these has the two solutions ± 1 , giving a total of 8 combinations. We need to explicitly compute the CRT map $g: \mathbf{Z}_{5^2} \times \mathbf{Z}_{17} \times \mathbf{Z}_{23} \rightarrow \mathbf{Z}_{9775}$, which we can do from the method of homework problem 3.24. Using the notation of that problem, $m_1 = 25$, $m_2 = 17$, $m_3 = 23$, and so $z_1 = 17 \cdot 23$, $z_2 = 25 \cdot 23$, and $z_3 = 25 \cdot 17$. Then, using the Euclidean algorithm 3 times we compute

$$y_1 = z_1^{-1} \pmod{m_1} = 391^{-1} \pmod{25} = 11$$

$$y_2 = z_2^{-1} \pmod{m_2} = 575^{-1} \pmod{17} = 11$$

$$y_3 = z_3^{-1} \pmod{m_3} = 425^{-1} \pmod{23} = 21$$

So,

$$g(a, b, c) \equiv ay_1z_1 + by_2z_2 + cy_3z_3 \equiv 4301a + 6325b + 8925c \pmod{9775}$$

Now we compute the 8 values:

$$g(1, 1, 1) = 1$$

$$g(1, 1, -1) = 1701$$

$$g(1, -1, 1) = 6901$$

$$g(1, -1, -1) = 8601$$

$$g(-1, 1, 1) = 1174$$

$$g(-1, 1, -1) = 2874$$

$$g(-1, -1, 1) = 8074$$

$$g(-1, -1, -1) = 9774$$