9 Tutorial 9 – November 28th, 2017

Midterm test.

9.1 Calculate 5^{676} in $(\mathbb{Z}_{306}, \cdot, 1)$ and use it to find all elements $x \in \mathbb{Z}_{306}$ for which

$$5^{676} \cdot x = 3\,(2x+1) \quad \text{in } (\mathbb{Z}_{306}, \cdot, 1).$$

Solution. We know that if a and n are relatively prime then $a^{\phi(n)} = 1$ in $(\mathbb{Z}_n, \cdot, 1)$. Since 5 and 306 are relatively prime and since

$$\phi(306) = \phi(2 \cdot 9 \cdot 17) = \phi(2) \cdot \phi(3^2) \cdot \phi(17) = 6 \cdot 16 = 96,$$

we have $5^{96} = 1$. So

$$5^{676} = 5^{7 \cdot 96 + 4} = 5^4.$$

Further, $5^4 = 13$ in $\mathbb{Z}_{306}$. Therefore, we obtain the following equation

$$13\,x = 6\,x + 3, \;\text{ hence }\; 7\,x = 3.$$

Solving the equation above, we get $x = 219$.

9.2 In $\mathbb{Z}_{148}$ the following equation with parameter p is given

$$p\,x - 5^{509} = 9\,x + 7.$$

a) Find all parameters p for which the equation above has a unique solution.

b) Solve the equation above for three such parameters (from a)).

Solution.
a) The equation above can be rewritten

$$(p-9)\,x = 5^{509} + 7,$$

and it has a unique solution if and only if $(p-9)$ is invertible in $(\mathbb{Z}_{148}, \cdot, 1)$. There are $\phi(148)$ distinct elements in $(\mathbb{Z}_{148}, \cdot, 1)$ that are invertible. Moreover,

$$\phi(148) = \phi(4) \cdot \phi(37) = 2 \cdot 36 = 72.$$

Hence, there are 72 distinct parameters in $\mathbb{Z}_{148}$ for which the above equation has a unique solution.

b) Since 5 and 148 are relatively prime, $5^{72} = 1$ in $\mathbb{Z}_{148}$. Therefore,

$$5^{509} = 5^{72 \cdot 7 + 5} = 5^5 = 17.$$

Therefore, the equation above is $(p-9)\,x = 24$ and the unique solutions will be $x = (p-9)^{-1} \cdot 24$ in $(\mathbb{Z}_{148}, \cdot, 1)$.

For example, we choose the following three parameters so that

$$p_1 - 9 = 1,\; p_2 - 9 = -1,\; p_3 - 9 = 3.$$

Hence, $p_1 = 10$, $p_2 = 8$, and $p_3 = 12$.

Therefore, for $p_1 = 10$ we get $x_1 = 24$, and for $p_2 = 8$ we get $x_2 = -24 = 124$.

For $p_3 = 12$ the easiest way is: since $3\,x = 24$ and 3^{-1} exists in $(\mathbb{Z}_{148}, \cdot, 1)$ we can cancel by 3 and get $x = 8$. Hence, $x_3 = 8$.