Mandatory Excercise 7

Computationally hard problems

November 15, 2015

Troels Thomsen 152165
Solution discussed with Rasmus Haarslev 152175

1 Excercise 7.4

In order to show the Jacobi symbol of $\left[\frac{773}{1373}\right]$ we follow the rules outlined in the lecture notes Theorem 5.23. We note that we are also given that $gcd(773, 1373) = 1$.

On the left side of the : we have which rule we utilized, and on the right side the calculation and result.

$$
\begin{aligned}
I3: \quad & (-1)^{\frac{772}{2}\times\frac{1372}{2}}\left[\tfrac{1373}{773}\right] && = \left[\frac{1373}{773}\right] && (1)\\
I2: \quad & 1373 \bmod 773 && = \left[\frac{600}{773}\right] && (2)\\
I1: \quad & \left[\tfrac{300}{773}\right]\left[\tfrac{2}{773}\right] && = \left[\frac{300}{773}\right](-1) && (3)\\
I1: \quad & \left[\tfrac{150}{773}\right](-1)\times\left[\tfrac{2}{773}\right] && = \left[\frac{150}{773}\right] && (4)\\
I1: \quad & \left[\tfrac{75}{773}\right]\times\left[\tfrac{2}{773}\right] && = \left[\frac{75}{773}\right](-1) && (5)\\
I3: \quad & (-1)(-1)^{\frac{74}{2}\times\frac{772}{2}}\left[\tfrac{773}{75}\right] && = \left[\frac{773}{75}\right](-1) && (6)\\
I2: \quad & 773 \bmod 75 && = \left[\frac{23}{75}\right](-1) && (7)\\
I3: \quad & (-1)^{\frac{22}{2}\times\frac{74}{2}}\left[\tfrac{75}{23}\right] && = \left[\frac{75}{23}\right] && (8)\\
I2: \quad & 75 \bmod 23 && = \left[\frac{6}{23}\right] && (9)\\
I1: \quad & \left[\tfrac{3}{23}\right]\times\left[\tfrac{2}{23}\right] && = \left[\frac{3}{23}\right] && (10)\\
I3: \quad & (-1)^{\frac{2}{2}\times\frac{22}{2}}\left[\tfrac{23}{3}\right] && = \left[\frac{23}{3}\right](-1) && (11)\\
I2: \quad & 23 \bmod 3 && = \left[\frac{2}{3}\right](-1) && (12)\\
I5: \quad & 3 \bmod 8 && = 1 && (13)
\end{aligned}
$$

We see that the Jacobi symbol for $\left[\frac{773}{1373}\right]$ is 1.