Math 153
Spring 2020
R. Schultz

SOLUTIONS TO EXERCISES FROM `math153exercises06X.pdf`

1. These numbers are still small enough that we can use *ad hoc* methods to find the answers.

(a) We have that $101 \equiv 4 \bmod 97$, so we want to find c such that $4c \equiv 1 \bmod 97$. The idea is to take some multiple of 4 which is close to 97. But $96 = 32 \times 4$, so $32 \times 4 \equiv -1 \bmod 97$, and this means that $(-32) \times 4 \equiv 1 \bmod 97$. Since $-32 \equiv 97 - 32 = 65$, it follows that $c = 65$.■

(b) We have that $101 \equiv 2 \bmod 99$, so we want to find c such that $2c \equiv 1 \bmod 99$. In this case we have $2 \times 50 = 100 \equiv 1 \bmod 99$. Therefore $c = 50$.■

(c) We now have that $101 \equiv -2 \bmod 103$. Since $2 \times 52 = 104 \equiv 1 \bmod 103$ it follows that we must have $c \equiv -52 \bmod 103$, and hence $c = 103 - 52 = 49$.■

(d) We have that $101 \equiv -4 \bmod 105$. Since $4 \times 26 = 104 \equiv -1 \bmod 105$ it follows that we must have $c \equiv -26 \bmod 105$, and hence $c = 105 - 26 = 79$.■

2. (a) We know that $(a+b\sqrt{p}) \cdot (a-b\sqrt{p}) \;=\; a^2 - pb^2 = N(a+b\sqrt{p})$. If this is zero then as in `history06b.pdf` we know that $a = b = 0$ by the irrationality of $\sqrt{p}$. Furthermore, we also have $N(a+b\sqrt{p}) \neq 0$ for the same reason. If we multiply $a+b\sqrt{p}$ by $(a-b\sqrt{p})/N(a+b\sqrt{p})$, the product is equal to 1, and therefore it follows that $(a-b\sqrt{p})/N(a+b\sqrt{p})$ is the reciprocal of $a+b\sqrt{p}$.■

(b) The equation $u^2 = v^2p - 1$ is equivalent to the norm equality $N(u+v\sqrt{p}) = -1$. Therefore if $a + b\sqrt{p} = (u + v\sqrt{p})^2$ we have

$$N(a+b\sqrt{p}) \;=\; N\left((u+v\sqrt{p})^2\right) \;=\; N(u+v\sqrt{p})^2 \;=\; (-1)^2 \;=\; 1$$

which is equivalent to $a^2 = b^2p + 1$.■