EXTRA HINTS FOR EXERCISE SHEET 5

Exercise 5.1. For $(\frac{2}{p})$, it will be easier if you consider 4 cases separately: $p \equiv 1, 3, 5$ or $7 \pmod 8$. For example, when $p \equiv 1 \pmod 8$, you can write $p = 8m + 1$ for some $m \geqslant 0$ and $r = 4m$. Then you need to explain why $2k$ has positive least residue for $1 \leqslant k \leqslant 2m$ and negative least residue for $2m + 1 \leqslant k \leqslant 4m$. You can analyse the other 3 cases in a similar way.

Exercise 5.2. Warning: this hint is really a spoiler which kills all the fun of this exercise. Stop reading if you want the full enjoyment in playing with the numbers.

All right. If you choose to continue reading, here are the secrets: in part (1) you can consider $N = 6p_1p_2 \cdots p_n - 1$, and in part (2) you can consider $M = (4q_1q_2 \cdots q_m)^2 - 2$. Note that 2 is a quadratic residue for any odd prime factor of M. Do not forget that M also has a prime factor 2.

Exercise 5.3. There is really nothing more that I can say. If you follow the hints and do everything correctly, at some point you will reach $2xc \equiv -b \pmod p$ which is an equation for c. Why does it have a solution for c?

Exercise 5.4. Assume that p is a prime in $\mathbb{Z}[i]$. If p divides $s^2 + 1 = (s + i)(s - i)$, then p must divide either $s + i$ or $s - i$, which means either $s + i$ or $s - i$ is the product of p and some other Gaussian integer. Why is this a contradiction?

Date: October 28, 2014.