Algebra II

Exercises for week 5

Note: Some problems might be hard – if you are stuck, you can find some hints in the textbook/online.

Problem 1. Prove on your own Wilson's theorem, ie. that for each p prime it is $(p-1)! \equiv -1 \pmod{p}$.

Problem 2. Show how it follows from Wilson's theorem that for each prime of the form $p = 4k+1$ the equation $x^2 = -1$ has a solution in the field $\mathbb{Z}_p$. (In number theory language, one can say this as "the number -1 is a quadratic residue modulo p")

Problem 3. Show that from the previous problem it follows that every prime $p = 4k+1$ is not irreducible in $\mathbb{Z}[i]$.

Problem 4. Show that from the previous problem it follows that a prime number can be written as $a^2 + b^2$ for $a, b \in \mathbb{Z}$ if and only if $p = 4k+1$.

Problem 5. Describe the irreducible (=prime, since $\mathbb{Z}[i]$ is Euclidean) elements of $\mathbb{Z}[i]$.

Problem 6. Use the previous problems to find a form for all the Pythagorean triples, ie. number $a, b, c \in \mathbb{Z}$ such that $a^2+b^2 = c^2$. Hint: Examine the problem in $\mathbb{Z}[i]$.

Problem 7. Solve the Diophantine equation not in your textbook, ie. one of:

1. $x^2 + 2 = y^3$,
2. $x^2 + 1 = y^3$.