Final Exam

1. (a) What is the norm of a gaussian integer? **(2 points)**

   (b) Prove that any gaussian integer divides its norm (among the gaussian integers). **(4 points)**

   Solution. (a) The norm of the gaussian integer $\alpha = a + b\sqrt{-1}$ (where $a, b \in \mathbf{Z}$) is defined as $N(\alpha) = a^2 + b^2$. Alternatively, using conjugates, we may define the norm to be $N(\alpha) = \alpha\overline{\alpha}$, where $\overline{\alpha} = a - b\sqrt{-1}$ is the conjugate of α.

   (b) Given a gaussian integer α, we have to check that there is a gaussian integer β such that $N(\alpha) = \alpha\beta$. Observe that $\beta = \overline{\alpha} = a - b\sqrt{-1}$ does this job: $\alpha\overline{\alpha} = N(\alpha)$, and $\overline{\alpha}$ is a gaussian integer, since $a, b \in \mathbf{Z}$ implies $a, -b \in \mathbf{Z}$.

2. (a) State Chebyshev's theorem about the number of primes up to a certain positive $x \geq 2$. **(2 points)**

   (b) Assume $p > q > 0$ are prime numbers such that $p + q$ and $p - q$ are also prime numbers. Give all the possibilities for the pair p, q. **(4 points)**

Solution. (a) Chebyshev's theorem: there exist positive constants c_1, c_2 such that for any $x \geq 2$,

$$c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x},$$

where $\pi(x)$ stands for the number of prime numbers not exceeding x.

(b) If $p > q > 2$, then p and q are odd primes, their sum is then an even number bigger than 2, so it cannot be prime. Therefore q must be 2.

Then if $p = 3$, then $p - q = 1$, which is not a prime.

If $p = 5$, then $p - q = 3$, $p + q = 7$, which are primes.

If $p > 5$, then modulo 3, p is either 1 or 2 (since it is a prime and exceeds 3, it cannot be divisible by 3). If $p \equiv 1 \bmod 3$, then $p + q \equiv 1 + 2 \equiv 0 \bmod 3$, and $p + q > 3$, which is hence not a prime. If $p \equiv 2 \bmod 3$, then $p - q \equiv 2 - 2 \equiv 0 \bmod 3$, and $p - q > 3$, which is hence not a prime.

Therefore the only solution is $p = 5, q = 2$.

3. (a) State the Euler-Fermat theorem. **(2 points)**

(b) Prove that there exist integers $100 < k < n$ such that $2^n - 2^k$ is divisible by 2017. **(4 points)**

Solution. (a) Euler-Fermat theorem: if a and $m \neq 0$ are coprime integers, then

$$a^{\varphi(m)} \equiv 1 \bmod m$$

where $\varphi(m)$ denotes the number of those residue classes modulo m which are coprime to m.

(b) Let k be any integer bigger than 100. Let then $n = k + \varphi(2017) > k > 100$. Then

$$2^n - 2^k = 2^{k+\varphi(2017)} - 2^k = 2^k(2^{\varphi(2017)} - 1),$$

and here, the second factor is divisible by 2017 by Euler-Fermat, since 2 is coprime to 2017.

Alternative solution to (b): consider all the numbers $2^{101}, 2^{102}, \ldots$. Since they are infinitely many, and there are only finitely many residue classes modulo 2017, there are two in the same residue class modulo 2017, let them be 2^k and 2^n (with $100 < k < n$). Then their difference is obviously divisible by 2017.

4. (a) Which integers can be represented as the sum of four squares? **(2 points)**

   (b) Prove that if a gaussian integer can be represented as the sum of some gaussian squares (squares of gaussian integers), then it can be represented as the sum of eight gaussian squares. **(4 points)**

Solution. (a) Every nonnegative integer can be written as the sum of four squares, this is the theorem on the sum of four squares.

(b) Assume $\alpha = a + b\sqrt{-1}$ be a gaussian integer (i.e. $a, b \in \mathbf{Z}$). Then $\alpha^2 = a^2 - b^2 + 2ab\sqrt{-1}$. This shows that the imaginary ('$\sqrt{-1}$') part of any gaussian square is even. Then this holds also for the sum of gaussian squares. Therefore a gaussian integer of odd imaginary part cannot be written as the sum of gaussian squares at all.

Therefore it suffices to show that any $\alpha = a + 2b\sqrt{-1}$ with $a, b \in \mathbf{Z}$ can be written as the sum of eight gaussian squares.

First we show that any $c \in \mathbf{Z}$ can be written as the sum of four gaussian squares. Indeed, if $c \geq 0$, then this follows from the theorem on four squares. While if $c < 0$, then $-c$ is the sum of four squares, again by the theorem on four squares, say, $-c = z_1^2 + z_2^2 + z_3^2 + z_4^2$, where $z_1, z_2, z_3, z_4 \in \mathbf{Z}$. Then

$$c = (z_1\sqrt{-1})^2 + (z_2\sqrt{-1})^2 + (z_3\sqrt{-1})^2 + (z_4\sqrt{-1})^2,$$

and $z_1\sqrt{-1}, z_2\sqrt{-1}, z_3\sqrt{-1}, z_4\sqrt{-1}$ are all gaussian integers.

Then applying this both to a and b, we have, for some gaussian integers $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$, that $a = x_1^2 + x_2^2 + x_3^2 + x_4^2$, $b = y_1^2 + y_2^2 + y_3^2 + y_4^2$. Then

$$\alpha = a + 2b\sqrt{-1} = (x_1^2 + x_2^2 + x_3^2 + x_4^2) + (y_1^2 + y_2^2 + y_3^2 + y_4^2)2\sqrt{-1}.$$

Observe that $2\sqrt{-1} = (1 + \sqrt{-1})^2$. This implies

$$\alpha = x_1^2 + x_2^2 + x_3^2 + x_4^2 + (y_1(1 + \sqrt{-1}))^2 + (y_2(1 + \sqrt{-1}))^2 + (y_3(1 + \sqrt{-1}))^2 + (y_4(1 + \sqrt{-1}))^2,$$

and here $x_1, x_2, x_3, x_4, y_1(1 + \sqrt{-1}), y_2(1 + \sqrt{-1}), y_3(1 + \sqrt{-1}), y_4(1 + \sqrt{-1})$ are all gaussian integers.