Mock Final Exam

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

   (b) Prove that for any gaussian integers α, β, we have $\overline{\alpha} + \overline{\beta} = \overline{\alpha + \beta}$ and $\overline{\alpha} \times \overline{\beta} = \overline{\alpha \times \beta}$. **(4 points)**

   Solution. (a) The conjugate of the gaussian integer $\alpha = a + b\sqrt{-1}$ (where $a, b \in \mathbf{Z}$) is defined as $\overline{\alpha} = a - b\sqrt{-1} = a + (-b)\sqrt{-1}$.

   (b) Let $\alpha = a + b\sqrt{-1}$, $\beta = c + d\sqrt{-1}$. Then

$$\overline{\alpha} + \overline{\beta} = a - b\sqrt{-1} + c - d\sqrt{-1} = (a + c) - (b + d)\sqrt{-1} = \overline{\alpha + \beta}.$$

   Also,

$$\overline{\alpha} \times \overline{\beta} = (a - b\sqrt{-1}) \times (c - d\sqrt{-1}) = (ac - bd) - (ad + bc)\sqrt{-1} = \overline{\alpha \times \beta}.$$

2. (a) What is the Pell equation? State the structure theorem about its solutions. **(2 points)**

(b) Give three solutions of the Pell equation $x^2 - 3y^2 = 1$ satisfying also $x, y > 0$. **(4 points)**

Solution. (a) By a Pell equation, we mean an equation of the form

$$x^2 - dy^2 = 1,$$

where $d > 0$ is an integer, which is not a square, and it is to be solved over the integers (in indeterminates x, y).

Theorem: there are infinitely many solutions and they can described as follows. There is a minimal solution among those where both $x_1, y_1 > 0$ (by minimal, we mean: minimal in x, or minimal in y, or minimal in $x + \sqrt{d}y$, these are all equivalent). Then take the numbers

$$x + \sqrt{d}y = \pm(x_1 + \sqrt{d}y_1)^n,$$

where n runs through the integers. This equation defines x and y up to sign: the 'integer' and the '$\sqrt{d}$ times integer' parts of $(x + \sqrt{d}y)^n$ give $\pm x$ and $\pm y$. Then these pairs x, y are solutions and these are all the solutions.

(b) There is a fundamental solution $x = 2, y = 1$: $2^2 = 4$, $3 \times 1^2 = 3 \times 1 = 3$.

Then a second solution can be computed as

$$(2 + \sqrt{3})^2 = 7 + \sqrt{3} \times 4,$$

and indeed, $x = 7, y = 4$ is a solution: $7^2 = 49$, $3 \times 4^2 = 3 \times 16 = 48$.

Then a third solution can be computed as

$$(2 + \sqrt{3})^3 = (7 + \sqrt{3} \times 4)(2 + \sqrt{3}) = 26 + \sqrt{3} \times 15,$$

and indeed, $x = 26, y = 15$ is a solution: $26^2 = 676$, $3 \times 15^2 = 3 \times 225 = 675$.

3. (a) In **Z**, what is the definition of prime numbers (the definition we used in the class)? In **Z**, what is the definition of irreducible numbers (the definition we used in the class)? What was proved about primes and irreducibles in **Z**? **(2 points)**

   (b) Give all positive integes n such that $n^3 - 27$ is a prime number. (Take care: although n is positive, $n^3 - 27$ can be negative, and there are negative primes!) **(4 points)**

Solution. (a) We say that an integer p different from 0 and ± 1 is a prime if the following holds: for any integers a, b, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

We say that an integer p different from 0 and ± 1 is irreducible if the following holds: for any integers a, b, if $p = ab$, then one of a and b is $\pm p$, the other one is ± 1.

In the class, we proved that in **Z**, prime numbers and irreducibles are the same.

(b) Observe that

$$n^3 - 27 = n^3 - 3^3 = (n-3)(n^2 + 3n + 3^2).$$

Here, if $n > 4$, then both $n - 3$ and $n^2 + 3n + 3^2$ are integers bigger than 1, so $n^3 - 27$ is not a prime.

If $n = 1$, then $n^3 - 27 = -26$, which is not a prime.

If $n = 2$, then $n^3 - 27 = -19$, which is a prime.

If $n = 3$, then $n^3 - 27 = 0$, which is not a prime.

If $n = 4$, then $n^3 - 27 = 37$, which is a prime.

So $n^3 - 27$ is a prime, if $n = 2, 4$.

4. (a) State the Chinese remainder theorem. **(2 points)**

   (b) Prove that there exist a positive integer n such that none of $n+1, \ldots, n+100$ is square-free. **(4 points)**

Solution. (a) Chinese remainder theorem: assume $m_1, \ldots, m_n$ satisfy $\gcd(m_i, m_j) = 1$ for all $1 \leq i < j \leq n$. Then for any $a_1, \ldots, a_n \in \mathbf{Z}$, there exists a unique residue class c modulo $m_1 \times \ldots \times m_n$ satisfying $c \equiv a_j \bmod m_j$ for each $1 \leq j \leq n$.

(b) Let $p_1, \ldots, p_{100}$ be pairwise different prime numbers. Then the numbers $p_1^2, \ldots, p_{100}^2$ are pairwise coprime. So by the Chinese remainder theorem, there is a positive integer (first a residue class, then any positive representative) satisfying

$$n \equiv -j \bmod p_j^2$$

for any $1 \leq j \leq 100$. Then for any $1 \leq j \leq 100$, $n+j$ is divisible by p_j^2, so none of $n+1, \ldots, n+100$ is square-free.