Exercise Sheet 3

For this exercise sheet, P will always denote a polynomial in $\mathbb{Z}[X]$, and we define the measure

$$\nu_q(a) = \frac{1}{q}|\{b \in \mathbb{Z}/q\mathbb{Z} | P(b) \equiv a \mod q\}|$$

on $\mathbb{Z}/q\mathbb{Z}$ for any positive integer q.

1. Show that for every function $f\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{R}$,

$$|\mathbb{E}(f(P(n) \mod q)) - \mathbb{E}_{\nu_q}(f)| \leq \frac{c\|f\|_1}{N},$$

for some constant c only depending on P.

2. Show that if $q = q_1 q_2$, with $(q_1, q_2) = 1$, then

$$\nu_q \text{ “=” } \nu_{q_1} \times \nu_{q_2},$$

i.e., show that for every $a \in \mathbb{Z}/q\mathbb{Z}$,

$$\nu_q(a) = \nu_{q_1}(a \mod q_1)\nu_{q_2}(a \mod q_2).$$

Hint: Use the Chinese remainder theorem.

3. Show that

$$\sum_{p \leq Q} \nu_p(0) = \log\log Q + O(1)$$

for $P(X) = X^2 + 1$.

Note: This actually holds for every monic and irreducible (over $\mathbb{Q}$) polynomial $P \in \mathbb{Z}[X]$.

4. a) Prove the following version of the Erdős-Kac theorem: For $N \geq 1$, let $\Omega_N = \{1, \ldots, N\}$ with the uniform probability measure $\mathbb{P}_N$. Let $P(X) = X^2 + 1 \in \mathbb{Z}[X]$ and let X_N be the random variable

$$n \mapsto \frac{\omega\big(P(n)\big) - \log \log N}{\sqrt{\log \log n}}$$

on Ω_N for $N \geq 3$. Then $(X_N)_{N \geq 3}$ converges in law to a standard normal random variable, i.e., to a normal random variable with expectation 0 and variance 1.

b) Prove a) for all monic and irreducible (over $\mathbb{Q}$) polynomials. Assume the result of exercise 3 for any monic and irreducible polynomial $P \in \mathbb{Z}[X]$.

Submission: Monday, 12th October 2015 during the exercise class.