Solution 3

1. We have

$$\begin{aligned}
\left|\mathbb{E}\big[f(P(n) \mod q)\big] - \mathbb{E}_{\nu_q}[f]\right| &= \left|\frac{1}{N}\mathbb{E}_{n\le N} f\big[\pi_q\big(P(n)\big)\big] - \sum_{a\in\mathbb{Z}/q\mathbb{Z}} \nu_q(a) f(a)\right| \\
&= \left|\frac{1}{N}\sum_{n\le N} f\big(\pi_q(P(n))\big) - \frac{1}{q}\sum_{b\in\mathbb{Z}/q\mathbb{Z}} f(P(b))\right| \\
&= \left|\frac{1}{N}\left\lfloor\frac{N}{q}\right\rfloor \sum_{0\le n<q} f\big(\pi_q(P(n))\big) - \frac{1}{q}\sum_{b\in\mathbb{Z}/q\mathbb{Z}} f(P(b))\right. \\
&\quad \left. + \frac{1}{N}\sum_{n=\left\lfloor\frac{N}{q}\right\rfloor q+1}^{N} f\big(\pi_q(P(n))\big)\right| \\
&\le \left|\Big(\frac{1}{N}\left\lfloor\frac{N}{q}\right\rfloor - \frac{1}{q}\Big)\sum_{b\in\mathbb{Z}/q\mathbb{Z}} f(P(b))\right| \\
&\quad + \frac{1}{N}\sum_{0\le n<q}\big|f\big(\pi_q(P(n))\big)\big| \\
&\le \frac{1}{N}\left|\sum_{b\in\mathbb{Z}/q\mathbb{Z}} f(P(b))\right| + \frac{1}{N}\sum_{0\le n<q}\big|f\big(\pi_q(P(n))\big)\big| \\
&\le \frac{2}{N}\sum_{b\in\mathbb{Z}/q\mathbb{Z}}\big|f(P(b))\big| \le \frac{2}{N}\deg(P)\sum_{a\in\mathbb{Z}/q\mathbb{Z}}\big|f(a)\big| \\
&\le \frac{2\deg(P)\|f\|_1}{N}.
\end{aligned}$$

2. This is an immediate consequence of the Chinese Remainder Theorem.

3. We first show that $x^2 + 1 \equiv 0 \mod p$ has two roots if $p \equiv 1 \mod 4$, one root if $p = 2$ and no roots if $p \equiv 3 \mod 4$.

Recall the following version/part of the quadratic reciprocity law: For $p \neq 2$, we have that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4, \\ -1 & \text{if } p \equiv 3 \mod 4. \end{cases}$$

Bitte wenden!

Hence -1 is a square modulo p if $p \equiv 1 \mod 4$, i.e., there exists x such that $x^2 \equiv -1 \mod p$. Since the multiplicative group $\mathbb{F}_p^\times$ is cyclic, it follows that every square in $\mathbb{F}_p^\times$ has exactly two roots. Hence the equation $-1 \equiv x^2 \mod p$ has exactly two solutions. The case $p \equiv 3 \mod 4$ is also covered by this discussion. For $p = 2$, it is easy to see that $x = 1$ is the only solution.

Now, we compute

$$\begin{aligned}\sum_{p \le Q} \nu_p(0) &= \nu_2(0) + \sum_{3 \le p \le Q} \nu_p(0) \\ &= \frac{1}{2} + 2 \sum_{\substack{p \le Q \\ p \equiv 1 \mod 4}} \frac{1}{p}\end{aligned}$$

which is by summation by parts

$$= 2\frac{\pi(Q;4,1)}{Q} + 2\int_2^Q \frac{\pi(t,4,1)}{t^2} dt + O(1)$$

and by the prime number theorem in arithmetic progressions, we get

$$\begin{aligned}&= \frac{2}{\varphi(4)\log Q} + \frac{2}{\varphi(4)}\int_2^Q \frac{1}{t\log t} dt + O(1) \\ &= \log\log Q + O(1).\end{aligned}$$

4. Part (a) follows immediately from part (b). The proof of part (b) is a direct adoption of the proof in the lecture notes which is done for the polynomial $P(X) = X$. One mainly has to replace n everywhere by $P(n)$ and make use of Exercises 1, 2 and 3 where appropriate.