Exercise Sheet 2

1. Let $f \in \mathbb{Z}[X]$ be a non-constant polynomial. Let p be a prime number and $\alpha \in \mathbb{Z}$ a root of f modulo p, so that $f(\alpha) \equiv 0 \bmod p$. The goal of this exercise is to prove one form of what is known as *Hensel's lemma*, which gives ways to "lift" roots of f modulo primes to roots modulo higher powers.

1. For any integer $k \geq 1$ and any $\beta \in \mathbb{Z}$, prove that

$$f(\alpha + p^k\beta) \equiv f(\alpha) + p^k\beta f'(\alpha) \bmod p^{k+1}.$$

Solution: The identity we want to prove is additive, so it suffices to prove it for monomials; that is, polynomials of the form $f(X) = cX^n$ for $c \in \mathbb{Z}$ and $n \in \mathbb{N}$, where n may be 0. Then

$$\begin{aligned} f(\alpha + p^k\beta) &\equiv c(\alpha + p^k\beta)^n \pmod{p^{k+1}}, \text{ by definition} \\ &\equiv c\alpha^n + c\sum_{j=1}^{n}\binom{n}{j}p^{jk}\beta^j\alpha^{n-j} \pmod{p^{k+1}}, \text{ by the binomial theorem.} \end{aligned}$$

If $k \geq 1$, then for any $j \geq 2$, $p^{jk} \equiv 0 \mod p^{k+1}$. Thus all terms in the sum vanish except for the $j = 1$ term, so that

$$\begin{aligned} f(\alpha + p^k\beta) &\equiv c\alpha^n + cnp^k\beta\alpha^{n-1} \pmod{p^{k+1}} \\ &\equiv f(\alpha) + p^k\beta f'(\alpha) \pmod{p^{k+1}}, \end{aligned}$$

as desired.

2. If p does not divide $f'(\alpha)$, prove that there exists $\beta \in \mathbb{Z}$ such that $f(\alpha + p\beta) \equiv 0 \bmod p^2$, and that β is unique modulo p.

Solution: Since $f(\alpha) \equiv 0 \mod p$, there exists some $m \in \mathbb{Z}$ with $f(\alpha) = pm$. Then by part (1), for all $\beta \in \mathbb{Z}$,

$$\begin{aligned} f(\alpha + p\beta) &\equiv f(\alpha) + p\beta f'(\alpha) \pmod{p^2} \\ &\equiv p(m + \beta f'(\alpha)) \pmod{p^2}. \end{aligned}$$

If $m + \beta f'(\alpha) \equiv 0 \mod p$, then $p(m + \beta f'(\alpha)) \equiv 0 \mod p^2$. Since $f'(\alpha) \not\equiv 0 \mod p$, it has an inverse modulo p; choosing any $\beta \in \mathbb{Z}$ with $\beta \equiv -mf'(\alpha)^{-1} \mod p$ will satisfy the desired constraint, and thus satisfy $f(\alpha + p\beta) \equiv 0 \mod p^2$. If $\beta \not\equiv -mf'(\alpha)^{-1} \mod p$, then $m + \beta f'(\alpha) \not\equiv 0 \mod p$. But in this case $f(\alpha + p\beta)$ is a nonzero multiple of p modulo p^2, and in particular $f(\alpha + p\beta) \not\equiv 0 \mod p^2$. Thus β is uniquely determined modulo p.

3. If p does not divide $f'(\alpha)$, prove that for any $k \geq 1$, there exists a unique root α_k of f in $\mathbb{Z}/p^k\mathbb{Z}$ such that $\alpha_k \equiv \alpha \bmod p$. Show also that $\alpha_l \equiv \alpha_k \bmod p^k$ if $l \geq k$.

   Solution: We proceed by induction, with the base case being that α is the unique root α_1 of f modulo p satisfying $\alpha_1 \equiv \alpha \mod p$.

   Assume that there exists a unique root α_k of f in $\mathbb{Z}/p^k\mathbb{Z}$ such that $\alpha_k \equiv \alpha \mod p$. We would like to construct the unique root $\alpha_k \in \mathbb{Z}/p^{k+1}\mathbb{Z}$. Let $\tilde{\alpha_k} \in \mathbb{Z}$ be the representative of $\alpha_k \bmod p^k$ with $0 \leq \tilde{\alpha_k} < p^k$.

   By part (1), we have for all $\beta \in \mathbb{Z}$ that

$$f(\tilde{\alpha_k} + p^k\beta) \equiv f(\tilde{\alpha_k}) + p^k\beta f'(\tilde{\alpha_k}) \mod p^{k+1}.$$

   Since α_k is a root of $f \bmod p^k$, we have $p^k | f(\tilde{\alpha_k})$; write $f(\tilde{\alpha_k}) = mp^k$. Then

$$f(\tilde{\alpha_k} + p^k\beta) \equiv p^k(m + \beta f'(\tilde{\alpha_k})) \mod p^{k+1}.$$

   As in part (2), the right-hand side is $0 \bmod p^{k+1}$ if and only if $m + \beta f'(\tilde{\alpha_k}) \equiv 0 \mod p$, which holds for a unique value $\beta \mod p$ since $f'(\tilde{\alpha_k}) \not\equiv 0 \mod p$. Call this value β_k and define

$$\alpha_{k+1} := \tilde{\alpha_k} + p^k\beta_k \mod p^{k+1}.$$

   By construction, $f(\alpha_{k+1}) \equiv 0 \mod p^{k+1}$ and $\alpha_{k+1} \equiv \alpha_k \equiv \alpha \mod p$. Moreover, by the uniqueness of α_k we must have $\alpha_{k+1} \equiv \alpha_k \mod p^k$; if not, $\alpha_{k+1} \mod p^k$ would be a second root of $f \mod p$. But then the uniqueness of α_{k+1} follows by the uniqueness of β_k.

   It remains to show that for $\ell \geq k$, $\alpha_\ell \equiv \alpha_k \mod p^k$. This follows inductively as well, since we have shown above that α_k is unique and that $\alpha_{k+1} \equiv \alpha_k \mod p^k$ for all k.

4. Find the unique element $\alpha \in \mathbb{Z}/17^3\mathbb{Z}$ such that $\alpha^2 = -1$ and $\alpha \equiv 4 \mod 17$.

   Solution: Define $f(X) \in \mathbb{Z}[X]$ via $f(X) = X^2 + 1$. Note that $f'(X) = 2X \not\equiv 0 \mod 17$.

   First note that 4 satisfies $f(4) = 17 \equiv 0 \mod 17$.. We can follow the algorithm of parts (2) and (3), noting that $f'(4) = 8$. Thus for all $\beta \mod 17$,

$$\begin{aligned} f(4 + 17\beta) &\equiv f(4) + 17\beta f'(4) \mod 17^2 \\ &\equiv 17(1 + 8\beta) \mod 17^2. \end{aligned}$$

   We have $1 + 8\beta \equiv 0 \mod 17$ if and only if $\beta \equiv 2 \mod 17$, so choosing $\beta = 2$ we have $f(\alpha_2) \equiv 0 \mod 17^2$ for $\alpha_2 \equiv 4 + 2 * 17 = 38 \mod 17^2$. Note that $f(38) = 1445 = 5 * 17^2$.

   We now repeat. For all $\beta \mod 17$,

$$\begin{aligned} f(38 + 17^2\beta) &\equiv f(38) + 17^2\beta f'(38) \mod 17^3 \\ &\equiv 17^2(5 + f'(38)\beta) \mod 17^3. \end{aligned}$$

   We have $5 + f'(38)\beta \equiv 0 \mod 17$ if and only if $5 + f'(4)\beta \equiv 5 + 8\beta \equiv 0 \mod 17$, which occurs if and only if $\beta \equiv 10 \mod 17$. Thus $\alpha_3 \mod 17^3$ given by $\alpha_3 = 38 + 10 * 17^2 = 2928$ satisfies $\alpha_3^2 \equiv -1 \mod 17^3$.

2. Let p be an odd prime number.

1. For $a \in \mathbb{Z}/p\mathbb{Z}$, show that
$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p.$$
(Hint: note that the right-hand side is always 0, 1 or -1, then distinguish cases according to the value of the Legendre symbol.)
Solution: Assume first that $\left(\frac{a}{p}\right) = 0$. Then $a \equiv 0 \mod p$, so $a^{(p-1)/2} \equiv 0 \mod p$, and equality holds.
Now assume that $\left(\frac{a}{p}\right) = \pm 1$. Consider the polynomial $f(X) = X^{p-1} - 1$. Note that for all $a \not\equiv 0 \mod p$, $a^{p-1} \equiv 1 \mod p$, since $(\mathbb{Z}/p\mathbb{Z})^\times$ is a group of order $p-1$. Thus every nonzero $a \mod p$ is a root of $f \mod p$. The polynomial f factors as $f(X) = (X^{(p-1)/2} - 1)(X^{(p-1)/2} + 1)$.
If $\left(\frac{a}{p}\right) = 1$, then for some $b \mod p$, $b^2 \equiv a$. Then
$$a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \mod p,$$
so in this case $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$, and a is a root of $X^{(p-1)/2} - 1 \bmod p$. There are precisely $(p-1)/2$ squares mod p and at most $(p-1)/2$ roots of $X^{(p-1)/2} - 1$ mod p, so the roots of $X^{(p-1)/2} - 1$ mod p must be precisely the squares mod p. Thus the roots of $X^{(p-1)/2} + 1$ must be precisely the remaining values (that is, nonsquares) mod p, so if $\left(\frac{a}{p}\right) = -1$, we have $a^{(p-1)/2} \equiv -1 \mod p$, which completes the argument.
2. Let a be coprime to p. For $1 \le b \le (p-1)/2$, let $\epsilon(b) \in \{-1, 1\}$ and $r(b) \in \{1, \dots, (p-1)/2\}$ be defined by the conditions that $ab \equiv \epsilon(b)r(b) \bmod p$. Show that $\epsilon(b)$ and $r(b)$ are uniquely defined and that the map r is injective. Deduce that
$$((p-1)/2)!a^{(p-1)/2} \equiv (-1)^\mu((p-1)/2)! \bmod p,$$
where μ is the number of integers b such that $\epsilon(b) = -1$.
Solution: Here we fix a coprime to p.
The map $\{-1, 1\} \times \{1, \dots, (p-1)/2\} \to (\mathbb{Z}/p\mathbb{Z})^\times$ given by $(\epsilon, r) \mapsto \epsilon r \mod p$ is bijective, since the values where $\epsilon = 1$ map bijectively onto $\{1, \dots, (p-1)/2\}$ and the values where $\epsilon = -1$ map bijectively onto $\{-1, \dots, -(p-1)/2\} \equiv \{p-1, \dots, p-(p-1)/2\} \mod p$; together these are precisely all nonzero values modulo p. Thus the values $\epsilon(b)$ and $r(b)$ are uniquely defined.
We now show that r is injective (and thus bijective, since it is a map from $\{1, \dots, (p-1)/2\}$ to itself). Let b_1 and b_2 be two values between 1 and $(p-1)/2$ and assume that $r(b_1) = r(b_2)$; call this value r. Then $ab_1 \equiv \epsilon(b_1)r \mod p$, so $ab_1\epsilon(b_1) \equiv r \mod p$ and similarly $ab_2\epsilon(b_2) \equiv r \mod p$. But then
$$\begin{aligned} ab_1\epsilon(b_1) &\equiv ab_2\epsilon(b_2) \mod p \\ \Rightarrow a(b_1\epsilon(b_1) - b_2\epsilon(b_2)) &\equiv 0 \mod p \\ \Rightarrow b_1\epsilon(b_1) - b_2\epsilon(b_2) &\equiv 0 \mod p, \text{ since } \gcd(a,p) = 1 \\ \Rightarrow b_1 &\equiv \epsilon(b_1)\epsilon(b_2)b_2 \mod p. \end{aligned}$$

Note that $\epsilon(b_1)\epsilon(b_2) = \pm 1$. Since each b_i satisfies $1 \leq b_i \leq (p-1)/2$, $b_1 \not\equiv -b_2 \mod p$. But then $b_1 \equiv b_2 \mod p$, so $b_1 = b_2$.

In order to deduce the desired equality we take the product over ab for all $1 \leq b \leq (p-1)/2$. We have

$$\prod_{b=1}^{(p-1)/2} ab = ((p-1)/2)! a^{(p-1)/2}$$

by definition of the factorial, but also

$$\prod_{b=1}^{(p-1)/2} ab \equiv \prod_{b=1}^{(p-1)/2} \epsilon(b) r(b) \equiv \prod_{b=1}^{(p-1)/2} \epsilon(b) \prod_{b=1}^{(p-1)/2} r(b) \mod p.$$

Since r is bijective, the product over $r(b)$ is also equal to $((p-1)/2)!$. The product over $\epsilon(b)$ has precisely μ values of (-1) and $(p-1)/2 - \mu$ values of 1, so the expression above is congruent to $(-1)^{\mu}((p-1)/2)!$, as desired.

3. Deduce that $(a/p) = (-1)^{\mu}$. (This is known as "Gauss's Lemma".)

   Solution: Since $((p-1)/2)!$ is relatively prime to p, the previous question implies that
   $$a^{(p-1)/2} \equiv (-1)^{\mu} \mod p.$$
   By part (1), $a^{(p-1)/2} \equiv (a/p) \mod p$, so $(a/p) = (-1)^{\mu}$.

4. Show that $(2/p) = 1$ if $p \equiv 1, 7 \mod 8$ and $(2/p) = -1$ otherwise. (Hint: use Gauss's Lemma, and consider the classes modulo 8 separately if needed to compute μ.)

   Solution: By Gauss's Lemma, $(2/p) = (-1)^{\mu}$, where μ is the number of integers $b \in [1, \frac{p-1}{2}]$ such that $2b \in [\frac{p+1}{2}, p-1]$, or equivalently such that $b \in [\frac{p+1}{4}, \frac{p-1}{2}]$.
   If $p \equiv 3 \mod 4$, then $\frac{p+1}{4}$ is an integer, so
   $$\mu = \frac{p-1}{2} - \frac{p+1}{4} + 1 = \frac{p+1}{4},$$
   which is even if $p \equiv 7 \mod 8$ and odd if $p \equiv 3 \mod 8$. If $p \equiv 1 \mod 4$, then $\frac{p+1}{4}$ is not an integer and $b \in [\frac{p+1}{4}, \frac{p-1}{2}]$ if and only if $b \in [\frac{p+3}{4}, \frac{p-1}{2}]$. Thus
   $$\mu = \frac{p-1}{2} - \frac{p+3}{4} + 1 = \frac{p-1}{4},$$
   which is even if $p \equiv 1 \mod 8$ and odd if $p \equiv 5 \mod 8$.
   Thus μ is even if $p \equiv 1, 7 \mod 8$ and odd if $p \equiv 3, 5 \mod 8$, so $(2/p) = (-1)^{\mu}$ is 1 if $p \equiv 1, 7 \mod 8$ and $(2/p) = -1$ if $p \equiv 3, 5 \mod 8$.

3. For $n \geq 1$, we denote by F_n the finite set of rational numbers of the form a/b where a and b are coprime and $0 \leq a \leq b \leq n$.

1. Write down F_5 as an ordered list of rational numbers. Do you notice anything about either successive elements $x < y$ of this list, or triples of successive elements $x < y < z$?

   Solution:

$$F_5 = \left\{ \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1} \right\}.$$

   This question will show that successive elements have relatively prime denominators, and that for successive elements $a/b < c/d < e/f$,

$$\frac{c}{d} = \frac{a+e}{b+f}.$$

2. Let $x = a/b$ be an element of F_n, with the conditions $1 \le a \le b \le n$, and a coprime to b. Show that there exists integers c and d such that $bc - ad = 1$, c and d are coprime and

$$0 \le n - b < d \le n.$$

   (Hint: start with any solution of $bc - ad = 1$, and adapt it to satisfy the inequality.)

   Solution: Since $\gcd(a, b) = 1$, by (for example) the Euclidean algorithm, there exist integers c and d such that

$$bc - ad = 1.$$

   Interpreting this equation as a linear combination of c and d, we see that $\gcd(c, d) | (bc - ad)$, and thus $\gcd(c, d) = 1$ for any such pair c and d.

   Note that if $bc - ad = 1$, then $b(c+a) - a(d+b) = 1$ and similarly $b(c-a) - a(d-b) = 1$. Thus for any $d' \equiv d \mod b$, there exists some c' with $bc' - ad' = 1$. Choosing d' to be the representative of d mod b with $n - b < d \le n$ gives the desired solution.

3. If $a/b < 1$, show that $c/d \in F_n$ and

$$\frac{c}{d} \ge \frac{a}{b}.$$

   Let e/f be the next element after a/b in F_n. Show that $c/d \ge e/f$, and that if $c/d > e/f$, then $c/d - e/f \ge 1/(df)$ and $e/f - a/b \ge 1/(bf)$.

   Solution: Since c and d are coprime, we need only show that $0 \le c \le d \le n$ in order to show that $\frac{c}{d} \in F_n$. Since $0 \le n - b < d \le n$, it remains only to show that $0 \le c \le d$, or equivalently that $0 \le c/d \le 1$.

   We can rearrange the identity $bc - ad + 1$ to get

$$\frac{c}{d} = \frac{a}{b} + \frac{1}{db}. \tag{1}$$

   Since $\frac{a}{b} < 1$, $\frac{a}{b} \le 1 - \frac{1}{b}$, so

$$\frac{c}{d} = \frac{a}{b} + \frac{1}{db} \le 1 - \frac{1}{b} + \frac{1}{db} \le 1,$$

   so $c/d \in F_n$. Equation (1) also implies immediately that $c/d \ge a/b$, and in fact that $c/d > a/b$.

Let e/f be the next element after a/b in F_n. Since $c/d > a/b$ is in F_n, by definition of e/f we must have $c/d \geq e/f$. Assume that $c/d > e/f$. Then

$$\frac{c}{d} - \frac{e}{f} = \frac{cf - de}{df} > 0,$$

so $cf - de > 0$ and thus $cf - de \geq 1$, which implies that $c/d - e/f \geq 1/(df)$. By the same argument, $e/f - a/b \geq 1/(bf)$.

4. Deduce that $c/d = e/f$ and that $be - af = 1$. (Hint: argue by contradiction using the two previous questions.)

<u>Solution:</u> Assume not. Then by part (3), $c/d > e/f$. Then part (3) implies that

$$\frac{bc - ad}{bd} = \frac{c}{d} - \frac{a}{b} = \left(\frac{c}{d} - \frac{e}{f}\right) + \left(\frac{e}{f} - \frac{a}{b}\right) \geq \frac{1}{df} + \frac{1}{bf} = \frac{b+d}{bdf}.$$

Clearing denominators from the far left and far right and applying the inequality from part (2) that $d > n - b$, we get that

$$bc - ad \geq \frac{b+d}{f} > \frac{b+n-b}{f} = \frac{n}{f} \geq 1,$$

where the last inequality follows since $e/f \in F_n$ and thus $f \leq n$. But then $bc - ad > 1$, which is a contradiction; thus $c/d = e/f$, so by part (2) we have $be - af = 1$.

5. Show that if $a/b < c/d < e/f$ are three successive elements in F_n, then

$$\frac{c}{d} = \frac{a+e}{b+f}.$$

(Hint: use twice the previous result, and compute c and d in terms of the other quantities.)

<u>Solution:</u> By the previous part we have $bc - ad = 1$ and $de - cf = 1$. Thus

$$\begin{aligned} bc - ad &= de - cf \\ \Rightarrow bc + cf &= de + ad \\ \Rightarrow c(b+f) &= d(a+e) \\ \Rightarrow \frac{c}{d} &= \frac{a+e}{b+f}, \text{ as desired.} \end{aligned}$$

(The set F_n is called the set of *Farey fractions* of order n; Farey himself did not have anything to do with proving the properties above.)

4. The goal of this exercise is to prove that π^2 is irrational. For $n \geq 0$, let

$$f_n = \frac{X^n(1-X)^n}{n!} \in \mathbb{Q}[X].$$

1. Show that for all $n \geq 1$ and $j \geq 0$, we have $f_n^{(j)}(0) \in \mathbb{Z}$ and $f_n^{(j)}(1) \in \mathbb{Z}$.

   Solution: We have $f_n(x) = \frac{r_n(x)s_n(x)}{n!}$, where $r_n(x) = x^n$ and $s_n(x) = (1-x)^n$. For each $j \geq 0$, by the product rule,

$$f_n^{(j)}(x) = \frac{1}{n!} \sum_{i=0}^{j} \binom{j}{i} r_n^{(i)}(x) s_n^{(j-i)}(x) \tag{2}$$

   (This is a generalization of the product rule which can be proven by induction). Then $r_n^{(i)}(x) = \frac{n!}{(n-i)!} x^{n-i}$ for $i \leq n$ and 0 otherwise, and $s_n^{(i)}(x) = (-1)^i \frac{n!}{(n-i)!}(1-x)^{n-i}$ for $i \leq n$ and 0 otherwise.

   Consider first the case when $x = 0$. Then $r_n^{(i)}(x) = 0$ unless $i = n$, so that $f_n^{(j)}(0) = 0$ when $0 \leq j \leq n-1$ and for $n \leq j \leq 2n$ we have

$$\begin{aligned}
f_n^{(j)}(0) &= \frac{1}{n!} \sum_{i=0}^{j} \binom{j}{i} r_n^{(i)}(0) s_n^{(j-i)}(0) \\
&= \frac{1}{n!} \binom{j}{n} r_n^{(n)}(0) s_n^{(j-n)}(0) \\
&= \frac{1}{n!} \binom{j}{n} \frac{n!}{0!} (-1)^{(j-n)} \frac{n!}{(2n-j)!} (1-0)^{j-2n} \\
&= \binom{j}{n} (-1)^{(j-n)} \frac{n!}{(2n-j)!}.
\end{aligned}$$

   Noting that $2n - j \leq n$ since $j \geq n$, this expression is an integer. Finally, for $n \geq 2j + 1$, every term in (2) is 0, so $f_n^{(j)}(x) = 0$ for these values.

   A similar computation for $x = 1$ shows that $f_n^{(j)}(1) = 0$ when $0 \leq j \leq n-1$ or when $j \geq 2n+1$, and that for $n \leq j \leq 2n$,

$$f_n^{(j)}(1) = \binom{j}{n} (-1)^{(j-n)} \frac{n!}{(2n-j)!} \in \mathbb{Z}.$$

2. Suppose that $\pi^2 = a/b$ where a and b are coprime positive integers. For $n \geq 1$, define $g_n \colon [0,1] \to \mathbb{R}$ by

$$g_n(x) = b^n \sum_{j=0}^{n} (-1)^j \pi^{2(n-j)} f_n^{(2j)}(x).$$

   Show that $g_n(0) \in \mathbb{Z}$ and $g_n(1) \in \mathbb{Z}$.

   Solution: We can write

$$g_n(x) = \sum_{j=0}^{n} (-1)^j b^n \left(\frac{a}{b}\right)^{n-j} f_n^{(2j)}(x) = \sum_{j=0}^{n} (-1)^j b^j a^{n-j} f_n^{(2j)}(x).$$

   By part (1), $f_n^{(2j)}(0) \in \mathbb{Z}$ and $f_n^{(2j)}(1) \in \mathbb{Z}$ for all $j \geq 0$, so when $x = 0$ or 1, every term in the sum for g_n is an integer, and thus $g_n(0) \in \mathbb{Z}$ and $g_n(1) \in \mathbb{Z}$.

3. Show that

$$g_n(0) + g_n(1) = \pi \int_0^1 a^n \sin(\pi x) f_n(x) dx.$$

(Hint: compute a primitive of $x \mapsto a^n \sin(\pi x) f_n(x)$ in terms of g_n.)

Solution: Define $F(x) = g_n'(x)\sin(\pi x) - g_n(x)\pi\cos(\pi x)$. Then

$$\begin{aligned} F'(x) &= g_n''(x)\sin(\pi x) + g_n'(x)\pi\cos(\pi x) - g_n'(x)\pi\cos(\pi x) + g_n(x)\pi^2\sin(\pi x) \\ &= \sin(\pi x) b^n \left(\sum_{k=0}^{n} (-1)^k \pi^{2(n-k)} f_n^{(2(k+1))}(x) + \sum_{j=0}^{n} (-1)^j \pi^{2(n-j+1)} f_n^{(2j)}(x) \right) \\ &= b^n \sin(\pi x) \left(\pi^{2(n+1)} f_n(x) + \sum_{j=1}^{n} \left((-1)^{j+1}\pi^{2(n-j+1)} f_n^{(2j)}(x) + (-1)^j \pi^{2(n-j+1)} f_n^{(2j)}(x) \right) \right), \end{aligned}$$

where in the last line we have isolated the $j = 0$ term from the second term, transformed the first sum via the substitution $j = k+1$, and discarded derivatives of f higher than the $2n$th derivative, at which point all derivatives of f are 0. The terms in the sum are all 0, so we get

$$\begin{aligned} F'(x) &= b^n \sin(\pi x)\pi^{2(n+1)} f_n(x) \\ &= \pi^2 a^n \sin(\pi x) f_n(x). \end{aligned}$$

Thus $\frac{1}{\pi}F(x)$ is the antiderivative of $\pi a^n \sin(\pi x) f_n(x)$, so that

$$\begin{aligned} \pi \int_0^1 a^n \sin(\pi x) f_n(x) \mathrm{d}x &= \frac{1}{\pi}(F(1) - F(0)) \\ &= \frac{1}{\pi}(g_n'(1)\sin(\pi) - g_n(1)\pi\cos(\pi) - g_n'(0)\sin(0) + g_n(0)\pi\cos(0) \\ &= g_n(0) + g_n(1), \end{aligned}$$

as desired.

4. Show that

$$0 < g_n(0) + g_n(1) < \frac{\pi a^n}{n!}$$

for all $n \geq 1$, and conclude.

Solution: For all $0 < x < 1$, we have $f_n(x) = \frac{x^n(1-x)^n}{n!} \leq \frac{1}{n!}$ and that $f_n(x)$ is nonnegative. The function $\sin(\pi x)$ also satisfies $0 \leq \sin(\pi x) \leq 1$ in the range $x \in [0,1]$, so

$$0 \leq \pi \int_0^1 a^n \sin(\pi x) f_n(x) \mathrm{d}x \leq \pi a^n \int_0^1 \frac{1}{n!} \mathrm{d}x = \frac{\pi a^n}{n!}.$$

Note also that $\sin(\pi x) = 0$ if and only if $x = 0$ or $x = 1$ in this range, and the same is true for $f_n(x)$; thus the integral is nonzero. Also, $\sin(\pi x) < 1$ for nearly the entire interval, so similarly the upper bound must be a strict upper bound. Combining this with part (3) completes the proof that $0 < g_n(0) + g_n(1) < \frac{\pi a^n}{n!}$ for all $n \geq 1$. Since $g_n(0) + g_n(1) \in \mathbb{Z}$ by part (2), this implies in turn that $\frac{\pi a^n}{n!} > 1$ for all $n \geq 1$. But for any fixed a, this quantity approaches 0 as $n \to \infty$, so we have reached a contradiction.

Due date: 14.10.2024