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
$$f(\alpha + p^k \beta) \equiv f(\alpha) + p^k \beta f'(\alpha) \bmod p^{k+1}.$$
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.
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 $l \geq k$.
4. Find the unique element $\alpha \in \mathbb{Z}/17^3\mathbb{Z}$ such that $\alpha^2 = -1$ and $\alpha \equiv 4 \bmod 17$.

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.)
2. Let a be coprime to p. For $1 \leq b \leq (p-1)/2$, let $\epsilon(b) \in \{-1, 1\}$ and $r(b) \in \{1, \ldots, (p-1)/2\}$ 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 $\epsilon(b) = -1$.
3. Deduce that $(a/p) = (-1)^{\mu}$. (This is known as "Gauss's Lemma".)
4. Show that $(2/p) = 1$ if $p \equiv 1, 7 \bmod 8$ and $(2/p) = -1$ otherwise. (Hint: use Gauss's Lemma, and consider the classes modulo 8 separately if needed to compute μ.)

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 $x < y < z$?
2. Let $x = a/b$ be an element of F_n, with the conditions $1 \leq a \leq b \leq n$, and a coprime to b. Show that there exists integers c and d such that $bc - ad = 1$, c and d are coprime and
$$0 \leq n - b < d \leq n.$$
(Hint: start with any solution of $bc - ad = 1$, and adapt it to satisfy the inequality.)
3. Show that $c/d \in F_n$ and
$$\frac{c}{d} \geq \frac{a}{b}.$$
Let e/f be the next element after a/b in F_n. Show that $c/d \geq e/f$, and that if $c/d > e/f$, then $c/d - e/f \geq 1/(df)$ and $e/f - a/b \geq 1/(bf)$.
4. Deduce that $c/d = e/f$ and that $be - af = 1$. (Hint: argue by contradiction using the two previous questions.)
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.)

(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 $f_n^{(j)}(1) \in \mathbb{Z}$.
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 $g_n(1) \in \mathbb{Z}$.
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.)

4. Show that
$$0 < g_n(0) + g_n(1) < \frac{\pi a^n}{n!}$$
for all $n \geq 1$, and conclude.

Due date: 14.10.2024