SOLUTION OF QUIZ 3, VERSION A, MATH100B, WINTER 2021

1. (5 points) Suppose n is a positive odd integer. Prove that $f(x) = (x-2)(x-4)\cdots(x-2n)-1 \in \mathbb{Q}[x]$ is irreducible.

   See the solution of Problem 4 of the week 6 HW assignment.

2. (5 points)Suppose $f, g \in \mathbb{Z}[x]$ are monic, p is prime, and $c_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ is the modulo-p residue map. Prove that if $\gcd(c_p(f), c_p(g)) = 1$ in $\mathbb{Z}_p[x]$, then $\gcd(f, g) = 1$ in $\mathbb{Q}[x]$.

   Suppose to the contrary that $\gcd(f, g) = q(x) \neq 1$. Let $\overline{q}(x), \overline{f}(x), \overline{g}(x) \in \mathbb{Z}[x]$ be the primitive forms of $q(x), f(x), g(x)$, respectively. Then by a result that we proved in class (see Proposition 14.1.3) we have $\overline{q}|\overline{f}$ in $\mathbb{Z}[x]$ and $\overline{q}|\overline{g}$ in $\mathbb{Z}[x]$ as $q|f$ in $\mathbb{Q}[x]$ and $q|g$ in $\mathbb{Q}[x]$. Notice that since f and g are monic, $\overline{f} = f$ and $\overline{g} = g$. So the integer polynomial $\overline{q}$ is a common divisor of the monic polynomials f and g. Hence there are $f_1, g_1 \in \mathbb{Z}[x]$ such that $f(x) = f_1(x)\overline{q}(x)$ and $g(x) = g_1(x)\overline{q}(x)$. Notice that since $f(x) = \overline{q}(x)f_1(x)$ and f is monic, the leading coefficient of $\overline{q}$ is ± 1. Hence $c_p(\overline{q})$ is a non-constant polynomial, $c_p(\overline{q})c_p(f_1) = c_p(f)$, and $c_p(\overline{q})c_p(g_1) = c_p(g)$. This means $\gcd(c_p(f), c_p(g)) \neq 1$, which is a contradiction.

   (See the solution of Problem 3 of the week 6 HW assignment.)

3. Suppose D is a PID and $I = \langle p \rangle$ is a non-zero prime ideal of D.

   (a) (5 points) Prove that p is an irreducible element of D.

   Since $\langle p \rangle$ is prime and $p \neq 0$, p is prime (see Lemma 13.2.3). Every prime is irreducible (see Lemma 13.3.2). Therefore p is irreducible.

   (b) (3 points) Prove that I is a maximal ideal of D.

   In a PID, p is irreducible exactly when $\langle p \rangle$ is maximal (see Lemma 9.3.2).

4. Suppose p is a prime, $a \in \mathbb{Z}_p^{\times}$, and $f(x) := x^p - x + a \in \mathbb{Z}_p[x]$. Suppose E is a field extension of $\mathbb{Z}_p$, and $\alpha \in E$ is a zero of $f(x)$. Notice that the characteristic of E is p.

   (a) (3 points) Prove that $x^p - x + a = (x - \alpha)\cdots(x - \alpha - (p-1))$ in $E[x]$.

   See the solution of Problem 3(a) of the week 5 HW assignment.

   (b) (5 points) Prove that $x^p - x + a \in \mathbb{Z}_p[x]$ is irreducible.

   See the solution of Problem 3(b) and 3(c) of the week 5 HW assignment.

   (c) (2 points) State the relevant results from the lectures or HW assignments and show that $\mathbb{Z}_p[\alpha]$ is a finite field of order p^p.

   Since $\alpha \in E$ is algebraic over $\mathbb{Z}_p$, $\mathbb{Z}_p[\alpha]$ is a field (see Theorem 9.4.1) and it is isomorphic to $\mathbb{Z}_p[x]/\langle m_{\alpha,\mathbb{Z}_p}(x)\rangle$ (see Equation (8.1)). Since α is a zero of the monic irreducible polynomial $x^p - x + a$, we have $m_{\alpha,\mathbb{Z}_p}(x) = x^p - x + a$ (see Theorem 8.2.4). By Problem 1 of the week 4 HW assignment, we have $|\mathbb{Z}_m[x]/\langle \sum_{i=0}^n a_i x^i \rangle| = m^n$ if $a_n \in \mathbb{Z}_m^{\times}$. Hence

   $$|\mathbb{Z}_p[\alpha]| = |\mathbb{Z}_p[x]/\langle x^p - x + a\rangle| = p^p.$$

(d) (2 points) Prove that $\prod_{a\in\mathbb{Z}_p^\times}(x^p - x + a)$ divides $x^{p^p} - x$.

Notice that $\alpha \in \mathbb{Z}_p[\alpha]^\times$ implies that $\alpha^{|\mathbb{Z}_p[\alpha]^\times|} = 1$. Hence α is a zero of $x^{p^p-1} - 1\mathbb{Z}_p[x]$, and so $m_{\alpha,\mathbb{Z}_p}(x) | x^{p^p-1} - 1$, which implies that $x^p - x + a | x^{p^p} - x$. We can deduce this result for every $a \in \mathbb{Z}_p^\times$ (it was OK to not say why, but can you make it precise) and these are distinct monic irreducible factors of $x^{p^p} - x$ in $\mathbb{Z}_p[x]$. Since $\mathbb{Z}_p[x]$ is a UFD, we deduce that $\prod_{a\in\mathbb{Z}_p^\times}(x^p - x + a)$ divides $x^{p^p} - x$.