Math 312- HW7 Due Date: 4/1/18

1. Prove that each of the following polynomials is irreducible in $\mathbb{Z}[x]$
   (a) $p(x) = x^4 + 12x^2 - 18x + 24$
   (b) $p(x) = 4x^3 + 15x^2 - 60x + 180$
   (c) $p(x) = 2x^5 + 25x^4 + 15x^3 + 30$
   (d) $p(x) = x^6 + x^3 + 1$ (Hint: evaluate $p(x+1)$)

   Solution:

   (a) $p(x) = x^4 + 12x^2 - 18x + 24$ is 3-Eisenstein so it is irreducible in $\mathbb{Q}[x]$. Since a greatest common divisor of the coefficients of the polynomial is 1 therefore $p(x)$ is also irreducible in $\mathbb{Z}[x]$
   (b) $p(x) = 4x^3 + 15x^2 - 60x + 180$ is 5-Eisenstein so it is irreducible in $\mathbb{Q}[x]$. Since a greatest common divisor of the coefficients of the polynomial is 1 therefore $p(x)$ is also irreducible in $\mathbb{Z}[x]$
   (c) $p(x) = 2x^5 + 25x^4 + 15x^3 + 30$ is 5-Eisenstein so it is irreducible in $\mathbb{Q}[x]$. Since a greatest common divisor of the coefficients of the polynomial is 1 therefore $p(x)$ is also irreducible in $\mathbb{Z}[x]$
   (d) Consider $p(x+1) = (x+1)^6 + (x+1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$. $p(x+1)$ is 3-Eisenstein so is irreducible in $\mathbb{Q}[x]$. Therefore $p(x)$ is irreducible in $\mathbb{Q}[x]$. Since a greatest common divisor of the coefficients of $p(x)$ is 1 therefore $p(x)$ is also irreducible in $\mathbb{Z}[x]$

2. Prove that the polynomial $p(x) = x^3 + x + 1$ is irreducible in $R = \mathbb{Z}/2\mathbb{Z}[x]$. Deduce that $R/\langle p(x)\rangle$ is a field and determine the size of this field.
   Solution:
   Since $\mathbb{Z}/2\mathbb{Z}$ is a field and $\deg p(x) = 3$ therefore to prove that $p(x)$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$ we only need to show that it has no roots in $\mathbb{Z}/2\mathbb{Z}$. Both $p(1) \neq 0$ and $p(0) \neq 0$ therefore $p(x)$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$. Since $\mathbb{Z}/2\mathbb{Z}$ is a field therefore $\mathbb{Z}/2\mathbb{Z}[x]$ is an Euclidean domain so is a PID. Recall that if S is a PID and $p \in S$ is irreducible then this is equivalent to p being a prime and also equivalent to $\langle p\rangle$ a prime ideal and furthermore equivalent to $\langle p\rangle$ being a maximal ideal. Therefore it follows that $\langle p(x)\rangle$ is a maximal ideal ideal of R which implies (since R is a commutative ring with unity) that $R/\langle p(x)\rangle$ is a field. The size of this field is $2^3 = 8$.

3. Find the irreducible factors of $x^8 - 1$ in $\mathbb{Q}[x]$
   Solution:
   We have
   $x^8 - 1 = (x^4 - 1)(x^4 + 1) = (x^2 - 1)(x^2 + 1)(x^4 + 1) = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$.We now show that each of the factors is irreducible in $\mathbb{Q}[x]$. Both $x - 1$ and $x + 1$ are clearly irreducible in $\mathbb{Q}[x]$. Since $\mathbb{Q}$ is a field and $\deg(x^2 + 1) = 2$ therefore to prove that it is irreducible we only have to prove that $x^2 + 1$ has no roots in $\mathbb{Q}$. Suppose that $\frac{r}{s} \in \mathbb{Q}$ is a root of $x^2 + 1$ where we assume that $\frac{r}{s}$ is in lowest terms. Then s divides the leading coefficient of $x^2 + 1$ which is 1 and r divides the constant term of $x^2 + 1$ which is also 1. This implies that $\frac{r}{s} = \pm 1$ and we see that both of these are not roots of $x^2 + 1$. This implies that $x^2 + 1$ is irreducible in $\mathbb{Q}[x]$. Now we check $p(x) = x^4 + 1$. We have $p(x + 1) = (x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$. This polynomial is 2-Eisenstein so is irreducible in $\mathbb{Q}[x]$. This then implies that $p(x) = x^4 + 1$ is irreducible in $\mathbb{Q}[x]$.

4. Find all monic irreducible polynomials of degree 2 in $\mathbb{Z}/3\mathbb{Z}[x]$.
   Solution:
   All monic polynomials in $\mathbb{Z}/3\mathbb{Z}[x]$ are of the form $x^2 + ax + b$ where $a, b \in \{0, 1, 2\}$. Since $\mathbb{Z}/3\mathbb{Z}$ is a field and the degree of the polynomial is 2 therefore such a polynomial will be irreducible if and only if the polynomial has no roots in $\mathbb{Z}/3\mathbb{Z}$ so we simply check all the possible monic polynomials of degree 2 for roots and we find that the ones that are irreducible are $p_1(x) = x^2 + 1$, $p_2(x) = x^2 + x + 2$ and $p_3(x) = x^2 + 2x + 2$

5. Find an infinite set of integers n such that the polynomial $p(x) = x^5 + 20x + n$ is irreducible in $\mathbb{Z}[x]$.
   Solution:
   Let $n = 2(2k + 1)$ where $k \in \mathbb{Z}$. For any such k the polynomial is 2-Eisenstein so is irreducible in $\mathbb{Q}[x]$. Since a greatest common divisor of the coefficients of the polynomial is 1, therefore the polynomial is also irreducible in $\mathbb{Z}[x]$.

6. Let I be the smallest ideal in $\mathbb{Z}[x]$ that contains 2 and x. Prove that I is not a principal ideal.
   Solution:
   Let $I = \{2f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$. We now show that I is in fact the smallest ideal containing 2 and x. First we show it is an ideal:
   (i) $0 = 2(0) + x(0) \in I$ so $I \neq \emptyset$
   (ii) Suppose that $p(x), q(x) \in I$. Then $p(x) = 2f(x) + xg(x)$, $q(x) = 2f'(x) + xg'(x)$ for some $f(x), f'(x), g(x), g'(x) \in \mathbb{Z}[x]$. Then
   $p(x) - q(x) = 2f(x) + xg(x) - (2f'(x) + xg'(x)) = 2(f(x) - f'(x)) + x(g(x) - g'(x)) \in I$
   (ii) Suppose that $p(x) \in I$ and $q(x) \in \mathbb{Z}[x]$. Then $p(x) = 2f(x) + xg(x)$ for some $f(x), g(x) \in \mathbb{Z}[x]$. We have $q(x)p(x) = 2q(x)f(x) + xq(x)g(x) \in I$. Since $\mathbb{Z}[x]$ is commutative we also have $p(x)q(x) \in I$.
   From (i), (ii) and (iii) I is an ideal of $\mathbb{Z}[x]$. Clearly I contains 2 and x. Now suppose that J is an ideal of $\mathbb{Z}[x]$ containing 2 and x. Let $f(x), g(x) \in \mathbb{Z}[x]$. Since J is an ideal of $\mathbb{Z}[x]$ therefore it contains $2f(x) + xg(x)$ which shows that $I \subseteq J$. This proves that I is the smallest ideal containing 2 and x.

   Suppose that I is principal. Then $I = \langle p(x) \rangle$ for some $p(x) \in \mathbb{Z}[x]$. Since $2 \in I$ therefore $2 = q(x)p(x)$ for some $q(x) \in \mathbb{Z}[x]$. This implies that $\deg p(x) = \deg q(x) = 0$ i.e. $p(x), q(x) \in \mathbb{Z}$ and so $p(x)$ divides 2 in $\mathbb{Z}$ so $p(x) = \pm 1, \pm 2$. If $p(x) \pm 1$ then $1 \in I$ and so $1 = 2f(x) + xg(x)$ for some $f(x), g(x) \in \mathbb{Z}[x]$ which is impossible. Therefore $p(x) = \pm 2$ so $I = \langle 2 \rangle = \langle -2 \rangle$. Since $x \in I$ therefore $x = 2f(x)$ for some $f(x) \in \mathbb{Z}[x]$ which is impossible. This proves that I is not principal.