PMTH332 Assignment 6

Jayden Turner (SN 220188234)

5 October 2018

Question 1

If ϕ is the Euler phi function, then we have $\phi(3) = 2$ and $\phi(5) = 4$. This, combined with Euler's theorem gives

$$a^2 \equiv 1 \mod 3 \tag{1}$$
$$b^4 \equiv 1 \mod 5 \tag{2}$$

where a and b are integers coprime to 3 and 5 respectively.

Take $n \in \mathbb{Z}$. If $3 \mid n$, then $n^{33} \equiv n \mod 3 \implies n^{33} - n \equiv 0 \mod 3$. Otherwise,

$$\begin{aligned} n^{33} - n = n(n^{32} - 1) &= n((n^2)^{16} - 1) \\ (1) \implies &\equiv n(1-1) \mod 3 \\ &\equiv 0 \mod 3 \end{aligned}$$

That is, for all $n \in \mathbb{Z}$, $3|n^{33} - n$. Likewise, if $5|n$, then $n^{33} \equiv n \mod 5 \implies n^{33} - n \equiv 0 \mod 5$. Otherwise,

$$\begin{aligned} n^{33} - n = n(n^{32} - 1) &= n((n^4)^{8} - 1) \\ (2) \implies &\equiv n(1-1) \mod 5 \\ &\equiv 0 \mod 5 \end{aligned}$$

That is, $5|n^{33} - n$ for all $n \in \mathbb{Z}$. Therefore, as both 3 and 5 divide $n^{33} - n$, and $\gcd(3,5) = 1$, it must hold that $3 \cdot 5 = 15|n^{33} - n$.

Question 2

Let F be a field. Then $F[x]$ is an integral domain permitting Euclidean function $d : F[x] \to \mathbb{N}$, where

$$d := \begin{cases} 0, & \alpha = 0 \\ 2^{\deg \alpha}, & \alpha \neq 0 \end{cases}$$

To see that this is a Euclidean function, we verify that d satisfies the three required axioms. Observe that E1 holds by definition, and that $d(1) = 2^{\deg 1} = 2^0 = 1$. Further, if $\alpha, \beta \in F[x]$ and $\beta \neq 0$, then $d(\alpha\beta) = 2^{\deg(\alpha\beta)} = 2^{\deg \alpha} 2^{\deg \beta} \geq 2^{deg \alpha} = d(\alpha)$ so E2 also holds. Finally, given arbitrary $\alpha, \beta in F[x]$ with expansions $\alpha = \sum_{i=0}^{n} a_i x^i$, $\beta = \sum_{j=0}^{m} b_j x^j$, where $n \geq m$, it is possible to define

$$q := \frac{a_n}{b_m} x^{n-m}$$

and

$$r := \alpha - q\beta \tag{3}$$

such that $\alpha = q\beta + r$. Expanding (3), we get

$$\begin{aligned}
\alpha - q\beta &= \sum_{i=0}^{n} a_i x^i - \frac{a_n}{b_m} x^{n-m} \sum_{i=0}^{m} b_i x^i \\
&= a_n x^n + \sum_{i=0}^{n-1} a_i x^i - a_n x^n - \sum_{i=n-m}^{n-1} \frac{a_n}{b_m} b_{i-n+m} x^i \\
&= \sum_{i=0}^{n-1} c_i x^i
\end{aligned}$$

with

$$c_i := \begin{cases} a_i, & 0 \leq i \leq n-m-1 \\ \frac{a_n}{b_m} b_i, & n-m \leq i \leq n-1 \end{cases}$$

Hence it is always possible to find q, r such that $\alpha = q\beta + r$ with $d(r) < d(\beta)$, and axiom E3 is satisfied. d is therefore a Euclidean function on integral domain $F[x]$, making $F[x]$ a Euclidean domain, and hence a principal ideal domain, by Theorem 17.3.

Take arbitrary prime ideal P of $F[x]$. As $F[x]$ is a pid, $P = (\alpha)$ for some $\alpha \in F[x]$, making α prime in $F[x]$ by definition. By Theorem 17.14, $(\alpha) = P$ must be maximal. Hence every prime ideal of $F[x]$, for field F, is maximal, as required.

Question 3

As shown in Question 2, if F is a field then $F[x]$ is a principal ideal domain. Therefore, as $\gcd(f(x), g(x)) = 1$, there exist $u(x), v(x) \in F[x]$ satisfying

$$1 = u(x)f(x) + v(x)g(x) \tag{4}$$

Given that $f(x) \mid h(x)$ and $g(x) \mid h(x)$, we have

$$h(x) = s(x)f(x) \tag{5}$$
$$h(x) = t(x)g(x) \tag{6}$$

for some $s(x), t(x) \in F[x]$. Multiply (4) by $h(x)$ to get

$$h(x) = u(x)h(x)f(x) + v(x)h(x)g(x) \tag{7}$$

Expanding $h(x)$ in the left summand with (6) and using (5) in the right, we obtain

$$\begin{aligned}
h(x) &= u(x)t(x)f(x)g(x) + v(x)s(x)f(x)g(x) \\
&= f(x)g(x)(u(x)t(x) + v(x)s(x))
\end{aligned}$$

and hence $f(x)g(x) \mid h(x)$ as required.

Question 4

a) As $\mathbb{Z}$ is principal ideal domain, so is $\mathbb{Z}_{12}$. That is, every ideal I is of the form $I = (a)$ for some $a \in \mathbb{Z}_{12}$. By Theorem 16.11, every non-zero maximal ideal of a commutative unital ring is prime. Therefore, it is possible to find the prime ideals of $\mathbb{Z}_{12}$ by finding the ideals generated by each element of $\mathbb{Z}_{12}$ and determining which are maximal. The ideals of $\mathbb{Z}_{12}$, excluding (0), are

$$\begin{aligned}
(1) &= \mathbb{Z}_{12} \\
(2) &= \{0, 2, 4, 6, 8, 10\} \\
(3) &= \{0, 3, 6, 9\} \\
(4) &= \{0, 4, 8\} \\
(5) &= \mathbb{Z}_{12} \\
(6) &= \{0, 6\} \\
(7) &= \mathbb{Z}_{12} \\
(8) &= \{0, 4, 8\} \\
(9) &= \{0, 3, 6, 9\} \\
(10) &= \{0, 2, 4, 6, 8, 10\} \\
(11) &= \mathbb{Z}_{12}
\end{aligned}$$

As prime ideals are, by definition, proper, we therefore have that the prime ideals of $\mathbb{Z}_{12}$ are (2) and (3).

b) $I = \mathbb{Z} \times \{0\}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$. To see that it is an ideal, take $(a, 0) \in I$ and $(b, c) \in \mathbb{Z} \times \mathbb{Z}$. Then $(a, 0) \cdot (b, c) = (ab, 0) \in I$. To see that it is prime, take $x = (a, b), y = (c, d) \in \mathbb{Z} \times \mathbb{Z}$. If $xy = (ac, bd)$ is in I, then either $c = 0$ or $d = 0$. Therefore $xy \in I$ implies $x \in I$ or $y \in I$, which makes I prime by definition. However, I is not maximal as $\mathbb{Z} \times p\mathbb{Z}$ is prime for prime integer p, and $I \subset \mathbb{Z} \times p\mathbb{Z}$.

Question 5

Evaluating $p(x) = x^3 + 2x + 3$ for each element of $\mathbb{Z}_5$ we get

$$\begin{aligned}
p(0) &\equiv 3 \\
p(1) &= 6 \equiv 1 \mod 5 \\
p(2) &= 15 \equiv 0 \mod 5 \\
p(3) &= 36 \equiv 1 \mod 5 \\
p(4) &= 75 \equiv 0 \mod 5
\end{aligned}$$

Hence $p(x)$ has roots in $\mathbb{Z}_5$ at $x = 2, 4$. By the factor theorem,

$$p(x) = (x-2)(x-4)\beta \equiv (x+3)(x+1)\beta$$

where β is an element of $\mathbb{Z}_5[x]$ of degree 1. Suppose $\beta = ax + b$. Then,

$$\begin{aligned}
p(x) = x^3 + 2x + 3 &= (ax+b)(x+3)(x+1) \\
&= (ax+b)(x^2 + 4x + 3) \\
&= ax^3 + (4a+b)x^2 + (3a+4b)x + 3b
\end{aligned}$$

Equating coefficients, we get $a = 1$ and $4 + b = 0 \implies b \equiv 1 \mod 5$. Therefore $p(x)$ can be decomposed into the product of irreducible polynomials

$$p(x) = (x+1)^2(x+3)$$