Math 116 Homework 5

Jerry Liu, 404474229

February 24, 2016

1 Homework Problems

Problem 1.

Proof.
Want to show that (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (1).
(1) $\Rightarrow$ (2) Suppose (1) is true. Let $ab = ac$ for some $a, b, c \in \mathrm{R}$. Assume $a \neq 0$.
$ab = ac \Leftrightarrow ab - ac = 0 \Leftrightarrow a(b - c) = 0$. By (1), since $a \neq 0$, $b - c = 0 \Leftrightarrow b = c$.

(2) $\Rightarrow$ (1) Assume (2) is true. Suppose $\exists\ a, b \in \mathrm{R}$, $a \neq 0, b \neq 0$ such that $ab = 0$.
Then $a \cdot b = 0 = a \cdot 0 \Rightarrow a \cdot b = a \cdot 0$. By (2), since $a \neq 0$, $b = 0$. Contradiction.
Similarly, since $b \neq 0$, By (2), $a = 0$. Contradiction.
Therefore $\forall\ a, b \in \mathrm{R}$, if $ab = 0$ then $a = 0$ or $b = 0$. $\square$

Problem 2.

Proof.
Reflexivity: $P(X) \mid 0 \Leftrightarrow P(X) \mid (A(X) - A(X)) \Leftrightarrow A(X) \equiv A(X) \pmod{P(X)}$
Symmetry: Suppose $A(X) \equiv B(X) \pmod{P(X)}$, $\Leftrightarrow P(X) \mid (A(X) - B(X))$
$\Leftrightarrow \exists\ Q(X) \in \mathrm{F}[X]$ such that $Q(X)P(X) = (A(X) - B(X))$.
Let $R(X) = -Q(X)$, then $R(X)P(X) = -Q(X)P(X) = -(A(X) - B(X)) = (B(X) - A(X))$
$\Leftrightarrow P(X) \mid (B(X) - A(X)) \Leftrightarrow B(X) \equiv A(X) \pmod{P(X)}$
Transitivity: Suppose $A(X) \equiv B(X) \pmod{P(X)}$ and $B(X) \equiv C(X) \pmod{P(X)}$
$\Leftrightarrow P(X) \mid (A(X) - B(X))$ and $P(X) \mid (B(X) - C(X))$
$\Leftrightarrow \exists\ M(X), N(X) \in \mathrm{F}[X]$ s.t. $M(X)P(X) = A(X) - B(X)$ and $N(X)P(X) = B(X) - C(X)$
Add two equations: $(M(X) + N(X))P(X) = A(X) - C(X) \Leftrightarrow P(X) \mid (A(X) - C(X))$
$\Leftrightarrow A(X) \equiv C(X) \pmod{P(X)}$
Therefore it is an equivalence relation. $\square$

Problem 3.

Proof.
We know $A_1(X) \equiv A_2(X) \pmod{P(X)}$ and $B_1(X) \equiv B_2(X) \pmod{P(X)}$
$\Rightarrow \exists\ M(X), N(X) \in \mathrm{F}[X]$ such that:

$$M(X)P(X) = A_1(X) - A_2(X) \tag{1}$$

$$N(X)P(X) = B_1(X) - B_2(X) \tag{2}$$

(a). $A_1(X) + B_1(X) \equiv A_2(X) + B_2(X) \pmod{P(X)}$
$(1) + (2)$: $M(X)P(X) + N(X)P(X) = A_1(X) - A_2(X) + B_1(X) - B_2(X)$
$\Leftrightarrow (M(X) + N(X))P(X) = (A_1(X) + B_1(X)) - (A_2(X) + B_2(X))$
$\Leftrightarrow P(X) \mid ((A_1(X) + B_1(X)) - (A_2(X) + B_2(X)))$
$\Leftrightarrow A_1(X) + B_1(X) \equiv A_2(X) + B_2(X) \pmod{P(X)}$

(b). $A_1(X) \cdot B_1(X) \equiv A_2(X) \cdot B_2(X) \pmod{P(X)}$
Want to show that $A_1(X) \cdot B_1(X) - A_2(X) \cdot B_2(X)$ is a multiple of $P(X)$.

$$\begin{aligned}
&A_1(X) \cdot B_1(X) - A_2(X) \cdot B_2(X) \\
&= A_1(X) \cdot B_1(X) - A_2(X) \cdot B_2(X) + A_1(X) \cdot B_2(X) - A_1(X) \cdot B_2(X) \\
&= A_1(X) \cdot B_1(X) - A_1(X) \cdot B_2(X) + A_1(X) \cdot B_2(X) - A_2(X) \cdot B_2(X) \\
&= A_1(X)(B_1(X) - B_2(X)) + B_2(X)(A_1(X) - A_2(X)) = A_1(X)N(X)P(X) + B_2(X)M(X)P(X) \\
&= (A_1(X)N(X) + B_2(X)M(X)) \cdot P(X)
\end{aligned}$$

$\Rightarrow P(X) \mid (A_1(X) \cdot B_1(X) - A_2(X) \cdot B_2(X))$
$\Leftrightarrow A_1(X) \cdot B_1(X) \equiv A_2(X) \cdot B_2(X) \pmod{P(X)}$ $\square$

Problem 4.

Solution.
Use Euclidean Algorithm to find out the greatest common divisor
Let $A(X) = 8X^4 - 12X^3 + 8X - 3$ and $B(X) = 4X^3 - 4X^2 - 3X + 2$ in $\mathbb{R}[X]$.
Note: $\deg(A(X)) > \deg(B(X))$.

$$\begin{aligned}
8X^4 - 12X^3 + 8X - 3 &= (4X^3 - 4X^2 - 3X + 2)(2X - 1) + (2X^2 + X - 1) \\
4X^3 - 4X^2 - 3X + 2 &= (2X^2 + X - 1)(2X - 3) + (2X - 1) \\
2X^2 + X - 1 &= (2X - 1)(X + 1) + 0
\end{aligned}$$

So gcd $= X - \frac{1}{2}$ since the leading coefficient needs to be *monic*

Problem 5.

Solution.
We know $A(X) = X^3 + 2X + 2$ and $B(X) = X^2 + 3X + 4$ in $\mathbb{F}_5[X]$.
By Extended Euclidean Algorithm:

$$\begin{aligned}
X^3 + 2X + 2 &= (X^2 + 3X + 4)(X + 2) + (2X + 4) \\
X^2 + 3X + 4 &= (2X + 4)(3X + 3) + (2) \\
3X + 3 &= (2)(4X + 4) + 0
\end{aligned}$$

So we can construct backwards:

$$\begin{aligned}
2 \cdot 3 = 1 &= 3((X^2 + 3X + 4) - (2X + 4)(3X + 3) = B(X) - (3X + 3)(A(X) - (X + 2)B(X))) \\
&= 3((2X + 2)A(X) + (1 + 3X^2 + X + 3X + 1)B(X)) \\
&= 3((2X + 2)A(X) + (3X^2 + 4X + 2)B(X)) \\
&= (X + 1)A(X) + (4X^2 + 2X + 1)B(X)
\end{aligned}$$

So when $P(X) = X + 1$ and $Q(X) = 4X^2 + 2X + 1$, $A(X)P(X) + B(X)Q(X) = 1$.

2 Book Problems

Problem. 21.
We know that 601 is a prime.

Part. a.

Proof.
Since $r < 600$ divides 600, $r = 2^a \cdot 3^b \cdot 5^c$ with $a \leq 3, b \leq 1, c \leq 2$
and these three can't be equal at the same time, otherwise $r = 600$. So we can split this in 3 cases:
If $a \leq 2$, then $r = 2^a \cdot 3^b \cdot 5^c$ with $a \leq 2, b \leq 1, c \leq 2 \Rightarrow r \mid 2^2 \cdot 3 \cdot 5^2 = 300$;
Similarly, if $b = 0$, $r \mid 2^3 \cdot 5^2 = 200$ and if $c \leq 1$, $r \mid 2^3 \cdot 3 \cdot 5 = 120$. $\square$

Part. b.

Proof.
By $20(e)$, we know $\text{ord}_{601}(7) \mid \phi(601) = 600 \Rightarrow$ by *part a*, $\text{ord}_{601}(7)$ divides one of $300, 200, 120$. $\square$

Part. c.

Proof.
From $20(d)$, we know $a^t \equiv 1 \pmod{601}$ if and only if $r = \text{ord}_{601}(7) \mid t$.
$7^{300}, 7^{200}, 7^{120}$ all do not congruent to $1 \pmod{601} \Rightarrow \text{ord}_{601}(7) \not| \, t$, where $t \in \{300, 200, 120\}$ $\square$

Part. d.

Proof.
By *part b, part c*, we know that $\text{ord}_{601}(7) \geq 600$. By $20(a)$, $\text{ord}_{601}(7) \leq \phi(601) = 600$.
$\Rightarrow \text{ord}_{601}(7) = 600 \Rightarrow 7^n \not\equiv 1 \pmod{601} \ \forall \ n < 600$.
$\Rightarrow \exists$ 600 distinct elements $\in \left\{1 = 7^{600}, 7^1, 7^2, ..., 7^{599}\right\} \pmod{601}$
$\Rightarrow 7$ is a primitive root $\pmod{601}$. $\square$

Part. e.

Solution.
If we want to check whether g is a primitive root $\pmod{p}$, we just check if:

$$
\begin{aligned}
&g^{\frac{n}{q_1}} \not\equiv 1 \pmod{p} \\
&g^{\frac{n}{q_2}} \not\equiv 1 \pmod{p} \\
&\cdots \\
&g^{\frac{n}{q_s}} \not\equiv 1 \pmod{p}
\end{aligned}
$$

where $n = p - 1$. If all the above holds, g is a primitive root $\pmod{p}$.

Problem. 22.
We know that $2^{32} \equiv 1 \pmod{65537}$, $2^{16} \not\equiv 1 \pmod{65537}$, $3^n \equiv 1 \pmod{65537}$ iff $65536 \mid n$.

Part. a.

Solution.
Want to find $k \in \mathbb{Z}$ such that $3^k \equiv 2 \pmod{65537}$.
First raise both sides by a power of 16: $3^{16k} \equiv 2^{16} \not\equiv 1 \pmod{65537}$
Then we raise both sides by a power of 32: $3^{32k} \equiv 2^{32} \equiv 1 \pmod{65537}$
$\Rightarrow 65536 \mid 32k$ but $65536 \not| \, 16k \Rightarrow 2048 \mid k$ but $4096 \not| \, k$ $\square$

Part. b.

Solution.
$2048 \mid k$ and $4096 \not| \, k$, and $k < 65536$. We know there are $65536/2048 = 32$ multiples of 2048 and all even multiples of 2048, multiples of 4096, is discarded.
$\Rightarrow$ There are 16 numbers that need to be tested.
We test 3^{2048i} for $i = 1, 3, 5, ..., 31$ such that $3^{2048i} \equiv 2 \pmod{65537}$.
After plugging into my computer program, when $i = 27$, $3^{2048 \cdot 27} \equiv 3^{55296} \equiv 2 \pmod{65537}$.

Problem. 33.

Part. a.

Proof.
For degree 1, $X, X + 1$ are the only polynomials of degree 1 in $\mathbb{Z}_2[X]$.
It suffices to show that they are irreducible.
For degree 2, possible polynomials are: $X^2, X^2 + 1, X^2 + X, X^2 + X + 1$,
but $X \cdot X \equiv X^2$, $(X + 1)^2 \equiv X^2 + 1$, and $X \cdot (X + 1) \equiv X^2 + X$. So only $X^2 + X + 1$ is irreducible.
Therefore, the only irreducible polynomials with degree < 2 in $\mathbb{Z}_2[X]$ are: $X, X + 1, X^2 + X + 1$. $\square$

Part. b.

Proof.
If $P(X) = X^4 + X + 1$ factors, it must have at least one factor of degree at most 2.
It suffices to show that $X \nmid P(X)$, and it can be shown that $X + 1 \nmid P(X)$ and remainder is 1;
$X^2 + X + 1 \nmid P(X)$ and the remainder is 1. Therefore $P(X)$ cannot be factored in $\mathbb{Z}_2[X]$. $\square$

Part. c.

Proof.
$X^4 - (X + 1) = X^4 + X + 1 \Leftrightarrow (X^4 + X + 1) \mid (X^4 - (X + 1)) \Leftrightarrow X^4 \equiv X + 1 \pmod{X^4 + X + 1}$
$\Rightarrow (X^4)^2 \equiv (X + 1)^2 \pmod{X^4 + X + 1} \Leftrightarrow X^8 \equiv X^2 + 2X + 1 \equiv X^2 + 1 \pmod{X^4 + X + 1}$
$\Rightarrow (X^8)^2 \equiv (X^2 + 1)^2 \pmod{X^4 + X + 1} \Leftrightarrow X^{16} \equiv X^4 + 2X^2 + 1 \equiv X^4 + 1 \equiv X \pmod{X^4 + X + 1}$ $\square$

Part. d.

Proof.
Since $X^4 + X + 1$ is irreducible in $\mathbb{Z}_2[X]$, and $\deg(X) < \deg(X^4 + X + 1)$, we can divide both sides by X:
$X^{16} \equiv X \pmod{X^4 + X + 1} \Rightarrow X^{15} \equiv 1 \pmod{X^4 + X + 1}$. $\square$

Problem. 34.

Part. a.

Proof.
Assume $X^2 + 1$ factors in $Z_3[X]$. $X^2 + 1$ has to have two factors of degree 1 polynomials.
In $Z_3[X]$, degree 1 polynomials are: $X, X+1, X+2$, but it suffices to show that none of them divides X^2+1.
Therefore it is irreducible in $Z_3[X]$. $\square$

Part. b.

Solution.
Use Euclidean Algorithm:

$$\begin{aligned} X^2 + 1 &= (2X + 1) \cdot (2X + 2) + 2 \\ 2X + 2 &= 2 \cdot (X + 1) + 0 \end{aligned}$$

Then we construct back:

$$\begin{aligned} 2 &= (X^2 + 1) \cdot 1 - (2X + 1) \cdot (2X + 2) \\ 2 &= (X^2 + 1) \cdot 1 + (2X + 1) \cdot (X + 1) \\ 1 = 2 \cdot 2 &= (X^2 + 1) \cdot 2 + (2X + 1) \cdot (2X + 2) \end{aligned}$$

Therefore the multiplicative inverse of $1 + 2X$ is $2X + 2$.

3 Source Code

`https://github.com/jerrylzy/Math116`