Homework 11

Jaden Wang

Problem (20.2)**.** Since 11 is prime, $\mathbb{Z}_{11}$ is a field, and $\phi(11) = 10$. Therefore, we are trying to find a generator from 1 to 10 that generates the group $U(\mathbb{Z}_{11})$ under $\times_{11}$. 7 happens to work:

$\times_{11}$	7	5	2	3	10	4	6	9	8	1

Thus, $\langle 7 \rangle = U(\mathbb{Z}_{11})$.

Problem (20.4)**.** By FlT, since 23 is prime, $3^{23-1} = 3^{22} \equiv 1 \bmod 23$.

$$\begin{aligned} 3^{47} &= 3^{44} \cdot 3^3 \\ &\equiv 1 \cdot 27 \bmod 23 \\ &\equiv 4 \bmod 23 \end{aligned}$$

Problem (20.5)**.** Since 7 is a prime, by FlT $37^6 = 1 \bmod 7$.

$$\begin{aligned} 37^{49} &= 37^{6\times 8} \cdot 37 \\ &\equiv 1 \cdot 37 \bmod 7 \\ &\equiv 2 \bmod 7 \end{aligned}$$

Problem (20.8)**.** Notice that since $\mathbb{Z}_{p^2}$ only has factor p which is prime, only multiples of p are not coprime with p^2 in $\mathbb{Z}_{p^2}$. There are $(p-1)$ such multiples in $\mathbb{Z}_{p^2}$. These multiples are the only zero divisors of $\mathbb{Z}_{p^2}$. Thus by theorem, the number of units are the group order of nonzero elements (p^2-1) subtracting the number of zero divisors $p-1$:

$$\phi(p^2) = (p^2-1) - (p-1) = (p+1)(p-1) - (p-1) = p(p-1).$$

Problem (20.10)**.** Since $\gcd(7, 24) = 1$, we can apply Euler and obtain $7^{23} = 1 \bmod 24$. Also notice $7^2 \bmod 24 = 1$, so 7 to the odd power mod 24 is 7. Therefore,

$$7^{1000} = 7^{43\times 23} \cdot 7^{11} \equiv 7 \bmod 24.$$

Problem (20.13)**.** $d = \gcd(36, 24) = 12$. Clearly d doesn't divide 15, so there is no solution by theorem.

Problem (20.14)**.** $d = \gcd(45, 24) = 3$. And $3/15$. Now let's divide everything by 3: $a' = \frac{45}{3} = 15, m' = \frac{24}{3}, b' = \frac{15}{3} = 5$. Thus we have

$$\begin{aligned} a'x &\equiv b' \bmod m' \\ 15x &\equiv 5 \bmod 8 \\ 8x + 7x &\equiv 5 \bmod 8 \\ 7x &\equiv 5 \bmod 8 \end{aligned}$$

The units in $\mathbb{Z}_8$ are 1,3,5,7. Notice $7 \times_8 7 \equiv 49 \bmod 8 \equiv 1 \bmod 8$. So 7 is its own inverse in $\mathbb{Z}_8$. Multiplying 7 on both sides:

$$\begin{aligned} 7 \times_8 7x &\equiv 7 \times_8 5 \\ x &\equiv 3 \end{aligned}$$

Problem (20.23)**.**

a) False. If $a = 0 \in \mathbb{Z}$, then $a^{p-1} \equiv 0 \bmod p$.

b) True.

c) True. Since $\mathbb{Z}_n$ has order n, the number of units must be less or equal to n.

d) False. If $n = 1$, then $\phi(n)$ is defined as $1 \neq 1 - 1 = 0$.

e) True. By theorem.

f) True. Given units $a, b \in \mathbb{Z}_n$, then $b^{-1}, a^{-1} \in \mathbb{Z}_n$, and the inverse of ab is $b^{-1}a^{-1} \in \mathbb{Z}_n$.

g) False. If $a, \in \mathbb{Z}_n$ are nonunits, then $\gcd(a, n) \neq 1$ and $\gcd(b, n) \neq 1$. It follows that $\gcd(ab, n) \neq 1$, which makes it not a unit.

h) False. By the same gcd argument as above.

i) False. Let $a = 0, b = 1$, $0x \equiv b \bmod p$ has no solution.

j) True. By theorem.

$\times_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Problem (20.24)**.** This is V_4 because all elements are their own inverses.

Problem (21.1)**.** We guess that $F = \{p+qi : p, q \in \mathbb{Q}\}$ is the field of fraction of D. Recall that we have shown in HW9 18.12 that structures similar to this is a field. Moreover, given $d = a + bi \in D$, $a, b \in \mathbb{Z} \subseteq \mathbb{Q}$, so $d \in F \Rightarrow D \subseteq F$. It remains to show that F is "not too big". That is, every element in F can be expressed as a fraction of two elements in D.

Given $\frac{r}{s} + \frac{t}{u}i \in F, r, s, t, u \in \mathbb{Z}, s, u \neq 0$, we have

$$\frac{r}{s} + \frac{t}{u}i = \frac{ru + sti}{su} = \frac{ru + sti}{su + 0i}.$$

Since $ru + sti, su + 0i \in D, s, u \neq 0 \Rightarrow su + 0i \neq 0$ since D has no zero divisors, this is indeed a well-defined fraction representation, as required.

Problem (21.2)**.** We guess that $F = \{p + q\sqrt{2} : p, q \in \mathbb{Q}\}$ is the field of fraction of D. Recall that we have shown in HW9 18.12 that this is a field. Moreover, given $d = a + b\sqrt{2} \in D$, $a, b \in \mathbb{Z} \subseteq \mathbb{Q}$, so $d \in F \Rightarrow D \subseteq F$. It remains to show that F is "not too big". That is, every element in F can be expressed as a fraction of two elements in D.

Given $\frac{r}{s} + \frac{t}{u}\sqrt{2} \in F, r, s, t, u \in \mathbb{Z}, s, u \neq 0$, we have

$$\frac{r}{s} + \frac{t}{u}i = \frac{ru + st\sqrt{2}}{su} = \frac{ru + st\sqrt{2}}{su + 0\sqrt{2}}.$$

Since $ru + st\sqrt{2}, su + 0\sqrt{2} \in D, s, u \neq 0 \Rightarrow su + 0\sqrt{2} \neq 0$ since D has no zero divisors, this is indeed a well-defined fraction representation, as required.

Problem (21.4)**.**

a) True.

b) False. $\mathbb{Q}$ is and field of fraction is unique up to isomorphism.

c) True. By theorem.

d) False. $\mathbb{R}$ is and it's unique up to isomorphism.

e) True. By theorem and uniqueness up to isomorphism.

f) True. The first time was for cancellation law to prove transitivity. The second time was for proving the 2nd element is non zero in addition and multiplication operations.

g) False. $0 \in D$ but 0 cannot be a unit.

h) True. By definition of a field and D is contained in F.

i) Since $D' \subseteq D \subseteq F$, so F is a field containing D'. Since F' is the smallest field containing D', it follows that $F' \leq F$.

j) True. Since it's unique up to isomorphism.

Problem (21.5)**.** Since $\mathbb{Q}$ is a field, it is also a domain by theorem. Let $D' = \mathbb{Z}$, and we know $\mathbb{Z} leq \mathbb{Q}$ is a subdomain. Moreover, we know $F' = \mathbb{Q}$, which is also the field of fractions of $\mathbb{Q}$ itself as required.