MODEL ANSWERS TO THE FIFTH HOMEWORK

3.2.2 Suppose that u_1 and u_2 are two units. Then there are two elements of the ring, v_1 and v_2, such that $u_1v_1 = 1 = u_2v_2$. We have

$$\begin{aligned}(u_1v_1)(u_2v_2) &= (u_1v_1)(u_2v_2)\\ &= 1\cdot 1\\ &= 1.\end{aligned}$$

Thus u_1u_2 is a unit. Thus the units are closed under multiplication and there is a well-defined multiplication of units. Multiplication of units is associative as multiplication in the ring is associative. 1 is a unit and it plays the role of the identity. If u is a unit then there is an element v of the ring such that $uv = 1$. Then u is the inverse of v in the ring, so that v is a unit. But then v is the inverse of u in the units, so that the units are a group.
3.2.2 Suppose that $a \equiv b \mod m$. Then m divides $a-b$ so that there is an integer k such that $a-b = mk$. Thus $a = b+mk$ and $b = a+(-k)m$. Suppose that d divides b and d divides m. Then d divides a and so d is a common divisor of a and m. Conversely if d divides a and m then it divides b and so d is a common divisor of b and m. Thus a, m and b, m have the same common divisors.
In particular they have the same greatest common divisor.
3.2.6 It is enough to show this for one common residue system. Consider

$$S = \{\, r \in \mathbb{Z} \mid -m/2 < r \leq m/2 \,\}$$

Then 1 and $-1 \in S$ and $1^2 = (-1)^2$.
3.2.7 If n is odd then

$$(-1)^{n/d} = -1,$$

for every divisor d of n. Therefore

$$\begin{aligned}\sum_{d|n}(-1)^{n/d}\varphi(d) &= \sum_{d|n} -\varphi(d)\\ &= -\sum_{d|n}\varphi(d)\\ &= -n.\end{aligned}$$

Now suppose that n is even. Then we may write $n = 2^k m$ where $k \geq 1$ and m is odd. If d is a divisor of n then $d = 2^j c$, where c is a divisor of m and $0 \le j \le k$. Note that c is odd. Therefore

$$\begin{aligned}
\sum_{d|n} (-1)^{n/d}\varphi(d) &= \sum_{j=0}^{k}\sum_{c|m}(-1)^{2^{k-j}m/c}\varphi(2^j c) \\
&= \sum_{c|m}\varphi(2^k)\varphi(c) - \sum_{j=0}^{k-1}\sum_{c|m}\varphi(2^j)\varphi(c) \\
&= \sum_{c|m}(2^k - 2^{k-1})\varphi(c) - \sum_{j=1}^{k-1}\sum_{c|m}(2^j - 2^{j-1})\varphi(c) - \sum_{k|m}\varphi(c) \\
&= (2^k - 2^{k-1})\sum_{c|m}\varphi(c) - \sum_{j=1}^{k-1}(2^j - 2^{j-1})\sum_{c|m}\varphi(c) - \sum_{k|m}\varphi(c) \\
&= (2^k - 2^{k-1})\varphi(m) - \sum_{j=1}^{k-1}(2^j - 2^{j-1})\varphi(m) - \varphi(m) \\
&= \varphi(m)(2^k - 2^{k-1} - \sum_{j=1}^{k-1}(2^j - 2^{j-1}) - 1) \\
&= \varphi(m)(2^k - 2^{k-1} - 2^{k-1}) \\
&= 0.
\end{aligned}$$

3.2.10 We apply the binomial theorem

$$\begin{aligned}
(a+b)^p &= a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \binom{p}{3}a^{p-3}b^3 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p \\
&\equiv a^p + b^p \mod p.
\end{aligned}$$

Here we used the fact that

$$\binom{p}{i} = \frac{p!}{i!(p-1)!}$$

is a natural number divisible by p, as neither $i!$ nor $(p-i)!$ are divisible by p.
It follows that

$$(a_1 + a_2 + a_3 + \cdots + a_n)^p \equiv a_1^p + a_2^p + \cdots + a_n^p \mod p$$

by induction on n. In particular

$$\begin{aligned} n^p &= (1+1+1+\cdots+1)^p \\ &\equiv 1^p + 1^p + \cdots + 1^p \mod p \\ &= 1+1+1+\cdots+1 \\ &= n. \end{aligned}$$

3.2.12 If $m = 1$ then $d = 1$ and in this case

$$\begin{aligned} \varphi(ab) &= \varphi(a)\varphi(b) \\ &= \frac{d\varphi(a)\varphi(b)}{\phi(d)}. \end{aligned}$$

By symmetry we are also done if $n = 1$. Thus we may assume that $m > 1$ and $n > 1$. Suppose that

$$m = p_1^{e_1} p_2^{e_2} \dots p_n^{e_t} \qquad \text{and} \qquad n = p_1^{f_1} p_2^{f_2} \dots p_n^{f_t}$$

are the prime factorisations of m and n. It follows that the prime factorisation of d is

$$n = p_1^{g_1} p_2^{g_2} \dots p_t^{g_t}$$

where $g_i = \min(e_i, f_i)$. In this case

$$\begin{aligned} \varphi(m) &= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \dots (p_t^{e_t} - p_t^{e_t-1}) \\ \varphi(n) &= (p_1^{f_1} - p_1^{f_1-1})(p_2^{f_2} - p_2^{f_2-1}) \dots (p_t^{f_t} - p_t^{f_t-1}) \\ \varphi(d) &= (p_1^{g_1} - p_1^{g_1-1})(p_2^{g_2} - p_2^{g_2-1}) \dots (p_t^{g_t} - p_t^{g_t-1}), \end{aligned}$$

where all products only run over the primes with non-zero indices. Since we can prove this formula prime by prime, we may assume that $m = p^e$ and $n = p^f$ where p is a prime and e and f are natural numbers. Possibly switching m and n we may assume that $e \leq f$. In this case $d = p^e$ and we have

$$\begin{aligned} \frac{d\varphi(a)\varphi(b)}{\phi(d)} &= \frac{p^e(p^e - p^{e-1})(p^f - p^{f-1})}{(p^e - p^{e-1})} \\ &= p^e(p^f - p^{f-1}) \\ &= p^{e+f} - p^{e+f-1} \\ &= \varphi(ab). \end{aligned}$$

3.2.14 Suppose that

$$n = p_1^{e_1} p_2^{e_2} \dots p_n^{e_t}$$

is the prime factorisation of n. It follows that the prime factorisation of d is

$$d = p_1^{f_1} p_2^{f_2} \dots p_t^{f_t}$$

where $f_i \leq e_i$. We have

$$\begin{aligned}\varphi(n) &= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \dots (p_t^{e_t} - p_t^{e_t-1}) \\ \varphi(d) &= (p_1^{f_1} - p_1^{f_1-1})(p_2^{f_2} - p_2^{f_2-1}) \dots (p_t^{f_t} - p_t^{f_t-1}).\end{aligned}$$

Therefore it suffices to observe that if p is a prime and $f \leq e$ are natural numbers then $p^f - p^{f-1} = p^{f-1}(p-1)$ divides $p^{e-1} - p^e = p^{e-1}(p-1)$.
3.2.23 We first find the prime factorisation of 561,

$$\begin{aligned}561 &= 3 \cdot 187 \\ &= 3 \cdot 11 \cdot 17.\end{aligned}$$

It follows that

$$a^2 \equiv 1 \mod 3 \qquad a^{10} \equiv 1 \mod 11 \qquad \text{and} \qquad a^{16} \equiv 1 \mod 17.$$

Note that 2, 10 and 16 all divide $2^4 \cdot 5 = 80$. Thus

$$a^{80} \equiv 1 \mod 3 \qquad a^{80} \equiv 1 \mod 11 \qquad \text{and} \qquad a^{80} \equiv 1 \mod 17.$$

It follows that $a^{80} - 1$ is divisible by 3, 11 and 17. As these numbers are coprime, it follows that $a^{80} - 1$ is divisible by $3 \cdot 11 \cdot 17 = 561$. Thus

$$a^{80} \equiv 1 \mod 561.$$

As $560 = 7 \cdot 80$, it follows that

$$\begin{aligned}a^{560} &= (a^{80})^7 \\ &\equiv 1^7 \mod 561 \\ &= 1.\end{aligned}$$

Suppose that m is not square free. Then there is a prime p such that p^2 divides m. We may write $m = p^e l$, where $e > 1$ and l is coprime to p. Consider

$$a = lp^{e-1} + 1.$$

We have

$$\begin{aligned}a^p &= (lp^{e-1} - 1)^p \\ &= (lp^{e-1})^p + \binom{p}{1}(lp^{e-1})^{p-1} + \dots + \binom{p}{1}(lp^{e-1}) + 1^p \\ &\equiv 1 \mod m.\end{aligned}$$

Thus a has order p.
Suppose that

$$a^{m-1} \equiv 1 \mod m.$$

Multiplying both sides by a we get

$$\begin{aligned} a &\equiv a^m \mod m \\ &= (a^p)^{lp^{e-1}} \\ &\equiv (1)^{lp^{e-1}} \mod m \\ &= 1. \end{aligned}$$

Thus $a \equiv 1 \mod m$, which is absurd.
Thus a^{m-1} is not equivalent, modulo m, to one.