Solutions to Problems in Abstract Algebra by Dummit and Foote (Chapter 0)

Isaac Dobes

0

0.1

0.1.1

Using the result from exercise 0.1.4 below, we conclude that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{B}$.

0.1.2

Recall that matrix multiplication is distributive. Therefore, $P, Q \in \mathcal{B} \iff MP = PM, MQ = QM \Rightarrow M(P + Q) = MP + MQ = PM + QM = (P + Q)M \Rightarrow P + Q \in \mathcal{B}$.

0.1.3

Recall that matrix multiplication is associative. Therefore, $P, Q \in \mathcal{B} \iff MP = PM, MQ = QM \Rightarrow M(P \cdot Q) = (M \cdot P)Q = (P \cdot M)Q = P(M \cdot Q) = P(Q \cdot M) = (P \cdot Q)M \Rightarrow P \cdot Q \in \mathcal{B}$.

0.1.4

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathcal{B} \iff \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \iff \begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix} = \begin{pmatrix} p & p+q \\ r & r+s \end{pmatrix} \iff$$

$$\begin{Bmatrix} p + r = p \\ q + s = p + q \\ r = r \\ s = r + s \end{Bmatrix} \iff \begin{Bmatrix} r = 0 \\ s = p \end{Bmatrix}$$

0.1.5

(a) There is some ambiguity in this question. Some define $\mathbb{Q}$ as $\{\frac{a}{a} : a, b \in \mathbb{Z}, b \neq 0, \text{ and } a \text{ and } b \text{ have no common divisors}\}$; in this case, $\frac{1}{2} \in \mathbb{Q}$, whereas $\frac{2}{4} \notin \mathbb{Q}$. If we accept this definition, then $f : \mathbb{Q} \to \mathbb{Z}$ defined as $f(\frac{a}{b}) = a$ is in fact well-defined since every rational number is uniquely determined by its numerator and denominator. If, however, we define $\mathbb{Q}$ as $\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$, then $f : \mathbb{Q} \to \mathbb{Z}$ defined as $f(\frac{a}{b}) = a$ is undefined since $\frac{1}{2} = \frac{2}{4}$, but $1 = f(\frac{1}{2}) \neq f(\frac{2}{4}) = 2$. Note that the book defines $\mathbb{Q}$ in the second way, so this is the answer I believe they are looking for; nonetheless, I think it is better to define $\mathbb{Q}$ in the first way.

(b) $f : \mathbb{Q} \to \mathbb{Q}$ defined as $f(\frac{a}{b}) = \frac{a^2}{b^2}$ is well-defined because if $\frac{a}{b} = \frac{c}{d}$, then $f(\frac{a}{b}) = \frac{a^2}{b^2} = (\frac{a}{b})^2 = (\frac{c}{d})^2 = f(\frac{c}{d})$.

0.1.6

The function $f : \mathbb{R}^+ \to \mathbb{Z}$ which maps a positive real number r to the first digit to the right of the decimal point in a decimal expansion of r is not well-defined since $0.999.... = 1.000....$, but $9 = f(0.999...) \neq f(1.000...) = 0$.

0.1.7

Given a surjective function $f : A \to B$, we want to prove that the relation $\sim$ on $A \times A$ defined as $a \sim b \iff f(a) = f(b)$ is an equivalent relation. Observe that:

(a) $a \sim a \iff f(a) = f(a)$, which indeed is always true (assuming f is a well-defined function); hence $\sim$ is reflexive

(b) $a \sim b \iff f(a) = f(b) \iff f(b) = f(a) \iff b \sim a$; hence, $\sim$ is symmetric

(c) $a \sim b, b \sim c \iff f(a) = f(b), f(b) = f(c) \iff f(a) = f(b) = f(c) \Rightarrow f(a) = f(b) \iff a \sim c$

Therefore, $\sim$ is an equivalence relation. Now, if $[a]$ is an equivalence class of $\sim$, then $b \in [a] \iff b \in A$ such that $f(a) = f(b) \Rightarrow [a] = f^{-1}(a)$; hence, the equivalence classes of $\sim$ are the fibers of f.

0.2

0.2.1

(a)

$$\begin{aligned}
20 &= 1(13) + 17 \\
13 &= 1(7) + 6 \\
7 &= 1(6) + 1 \\
6 &= 6(1)
\end{aligned}$$

$\Rightarrow \gcd(20, 13) = 1$. Since 20 and 13 are relatively prime, $\text{lcm}(20, 13) = 20(13) = 260$. Working backwards, we see that:

$$\begin{aligned}
1 &= 7 - 1(6) \\
&= 7 - 1[13 - 1(7)] \\
&= 2(7) - 13 \\
&= 2[20 - 1(13)] - 13 \\
&= 2(20) - 3(13)
\end{aligned}$$

$\Rightarrow \gcd(20, 13) = 2(20) - 3(13)$.

(b)

$$\begin{aligned}
372 &= 5(69) + 27 \\
69 &= 2(27) + 15 \\
27 &= 1(15) + 12 \\
15 &= 1(12) + 3 \\
12 &= 4(3)
\end{aligned}$$

$\Rightarrow \gcd(372, 69) = 3$. $\text{lcm}(372, 69) = \frac{372(69)}{\gcd(372,69)} = \frac{25,668}{3} = 8,556$. Working backwards, we see that:

$$\begin{aligned} 3 &= 15 - 1(12) \\ &= 15 - 1(27 - 15) \\ &= 2(15) - 27 \\ &= 2[69 - 2(27)] - 27 \\ &= 2(69) - 5(27) \\ &= 2(69) - 5[372 - 5(69)] \\ &= 27(69) - 5(372) \end{aligned}$$

$\Rightarrow \gcd(372, 69) = (-5)372 + (27)69$.

(c)

$$\begin{aligned} 792 &= 2(275) + 242 \\ 275 &= 1(242) + 33 \\ 242 &= 7(33) + 11 \\ 33 &= 3(11) \end{aligned}$$

$\Rightarrow \gcd(792, 275) = 11$. Now, $\text{lcm}(792, 275) = \frac{792(275)}{\gcd(792,275)} = \frac{217,800}{11} = 19,800$. Working backwards, we see that:

$$\begin{aligned} 11 &= 242 - 7(33) \\ &= 242 - 7[275 - 1(242)] \\ &= 8(242) - 7(275) \\ &= 8[792 - 2(275)] - 7(275) \\ &= 8(792) - 23(275) \end{aligned}$$

$\Rightarrow \gcd(792, 275) = 8(792) - 23(275)$.

(d) Omitted.

(e) Omitted.

Parts (d) and (e) are omitted because they are analogous to (a), (b), and (c).

0.2.2

We are told that $k|a$ and $k|b$, and we want to show that $k|(as + bt)$. Since $k|a$, there exists $c \in \mathbb{Z}$ such that $a = kc$; similarly, $k|b$ implies that there exists $d \in \mathbb{Z}$ such that $b = kd$. Therefore,

$$as + bt = kcs + kdt = k(cs + dt)$$

$\Rightarrow k|(as + bt)$.

0.2.3

We are told that n is composite and we want to show that there exists integers a and b such that $n|ab$ but $n \nmid a$ and $n \nmid b$. Now, $n = p_1^{\alpha_1} \cdot ... \cdot p_s^{\alpha_s}$, where $s \geq 1$, $\alpha_i \geq 1 \ \forall i \in [s]$, and $p_1, ..., p_s$ are prime. Let p be a prime number such that $p \notin \{p_1, ..., p_s\}$. Then $pn = p(p_1^{\alpha_1} \cdot ... \cdot p_s^{\alpha_s})$. Since n is composite, $p_1^{\alpha_1} \cdot ... \cdot p_s^{\alpha_s}$ is the product of two or more primes, which implies that we may be able to factor out p_1 from $p_1^{\alpha_1} \cdot ... \cdot p_s^{\alpha_s}$ to obtain $pn = pp_1(p_1^{\alpha_1 - 1} \cdot ... \cdot p_s^{\alpha_s})$; setting $a := pp_1$ and $b := p_1^{\alpha_1 - 1} \cdot ... \cdot p_s^{\alpha_s}$, we have $pn = ab$. $n \nmid a$ since $n = p_1 b$, $a = pp_1$, p is prime, and $b > 1$; moreover, $n \nmid b$ since $n > b$. Nonetheless, $n|ab$.

0.2.4

Given fixed integers a, b, and N, with $a, b \neq 0$, we are told that (x_0, y_0) is a solution to

$$ax + by = N \qquad (\star)$$

We want to show that for any $t \in \mathbb{Z}$, $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$ is also a solution. Observe that

$$\begin{aligned} a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) &= ax_0 + by_0 + \frac{ab}{d}t + by_0 - \frac{ba}{d}t \\ &= ax_0 + by_0 \\ &= N \end{aligned}$$

$\Rightarrow$ for any $t \in \mathbb{Z}$, $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$ is also a solution to $(\star)$.

0.2.5

We want to determine the value of $\phi(n)$ for each integer $n \leq 30$, where $\phi(\cdot)$ denotes the Euler ϕ-function. Recall that $p_1, ..., p_s$ prime,

$$\phi(p_1^{\alpha_1} \cdot ... \cdot p_s^{\alpha_s}) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot ... \cdot p_s^{\alpha_s - 1)(p_s - 1)}$$

Therefore,

$$\begin{aligned} \phi(1) &= 1 \\ \phi(2) &= 1 \\ \phi(3) &= 2 \\ \phi(4) &= 2^1(2-1) = 2 \\ \phi(5) &= 4 \\ \phi(6) &= 2^0(2-1)3^0(3-1) = 2 \\ \phi(7) &= 6 \\ \phi(8) &= 2^2(2-1) = 4 \\ \phi(9) &= 3^1(3-1) = 6 \\ \phi(10) &= 2^0(2-1)5^0(5-1) = 4 \\ \phi(11) &= 10 \\ \phi(12) &= 2^1(2-1)3^0(3-1) = 4 \\ \phi(13) &= 12 \\ \phi(14) &= 2^0(2-1)7^0(7-1) = 6 \\ \phi(15) &= 3^0(3-1)5^0(5-1) = 8 \end{aligned}$$

I will stop here because it is tedious and trivial computing the rest.

0.2.6

Let $\emptyset \neq A \subset \mathbb{N}$. We use strong induction to prove that A has a minimal element.
Base Case: Suppose $1 \in A$. Then clearly 1 is minimal in A.
Induction Hypothesis: Assume there exists some $k \in \{1, 2, ..., n\}$, and that A has a minimum element.
Induction Step: Now suppose there is an element $k \in A$ such that $k \in \{1, ..., n, n+1\}$. If $k \leq n$, then this case reduces to the induction hypothesis case, and we are done. If, on the other hand, $j \notin A$ for any positive integer $j \leq n$, then $(n+1) \in A$ is the minimal element in A.

NOTE: It is clear that if k is minimal in A, then k is the unique minimum in A since $m = \min(A) \iff m \leq x$ $\forall x \in A$; therefore, if k_1 and k_2 are minimal in A, then $(k_1 \leq k_2 \wedge k_2 \leq k_1) \iff k_1 = k_2$.
NOTE 2: Using induction yields an "awkward" proof. A much better approach to proving that A has a minimum element would be by constructing an algorithm, so I will present one here as an alternative proof.

Algorithm 1: MinA

```
Input: A non-empty set A ⊂ ℕ
Output: m, where m is the minimum element of A
i := 1;
if i ∈ A then
|   return i;
else
|   while i ∉ A do
|   |   i := i + 1;
|   end
|   return i;
end
```

Since $A \subset \mathbb{N}$ is non-empty, the algorithm will eventually terminate, and when it does, it will return the minimum element of A.

0.2.7

Assume for the sake of contradiction that there exists nonzero integers a and b such that $a^2 = pb^2$, where p is prime. Let $d = \gcd(a, b)$. Then setting $A := \frac{a}{d}$ and $B := \frac{b}{d}$, we have $A^2 = pB^2$; thus, there exists relatively prime integers A and B such that $A^2 = pB^2$. Now, $p|A^2 \iff p|(A \cdot A) \Rightarrow p|A$ since p is prime. This implies that $p^2|A^2 \iff p^2|pB^2 \Rightarrow p|B^2 \iff p|(B \cdot B) \Rightarrow p|B$. This contradicts the fact that A and B are relatively prime, thus implying that there does not that there does not exist nonzero integers a and b such that $a^2 = pb^2$, for any prime p.

0.2.8

Given p prime and $n \in \mathbb{N}$, we want to find a formula for the largest power d of p which divides $n!$. Observe that since $n! = n(n-1) \cdot ... \cdot (2)(1)$, we obtain atleast one factor of p in $n!$ for each multiple of p in $\{1, 2, ..., n\}$; there are precisely $\left\lfloor \frac{n}{p} \right\rfloor$ many multiples. Note, however, if $p^2 < n$, then p^2 contributes atleast one additional factor of p; more precisely, there are an additional $\left\lfloor \frac{n}{p^2} \right\rfloor$ many factors of p (one for each multiple of p^2 i $\{1, 2, ..., n\}$). We may continue on in this manner up to any arbitary power of k of p $\left(\text{even when } p^k > n, \text{ since } \left\lfloor \frac{n}{p^k} \right\rfloor = 0\right)$; thus, we have the formula

$$d = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

0.2.9

Omitted.

0.2.10

Let $\phi(n) = N$ for some $n \in \mathbb{N}$. If $n = p^{\alpha_1} \cdot ... \cdot p_s^{\alpha_s} = \prod_{i=1}^{s} p_i^{\alpha_i}$, where $\forall i \in [s]$, p_i is prime and $\alpha_i \in \mathbb{N}$, then we have:

$$\phi(n) = \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1) = N$$

$\Rightarrow$ the largest prime factor n may have is smaller than $N+1$, and for each p_i there is some positive integer exponent β_i such that $p_i^x > N$ for all positive integers $x \geq \beta_i$. Therefore, there are only finitely many choices of exponents for the finitely many prime factors of n so that $\phi(n) = N$. This implies that there are only finitely many n so that $\phi(n) = N$

Now assume for the sake of contradiction that the Euler ϕ-function is bounded. Then there exists $M \in \mathbb{N}$ such that $\phi(n) \leq M \ \forall n \in \mathbb{N}$. Since the codomain of the Euler ϕ-function is the set of positive integers, there must exist some $N \in [M]$ such that $|\phi^{-1}(N)| = \infty$ which contradicts the fact that there are only finitely many n such that $\phi(n) = N$, $\forall N \in \mathbb{N}$.

0.2.11

We are told that $d|n$ and we want to show that $\phi(d)|\phi(n)$. Since $d|n$, there exists $c \in \mathbb{Z}$ such that $n = cd$. Let $p_1^{\alpha_1} \cdot ... \cdot p_s^{\alpha_s}$ be the prime factorization of c. Then we have:

$$\phi(n) = \phi(cd) = \phi(p_1^{\alpha_1} \cdot ... \cdot p_s^{\alpha_s} d) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot ... \cdot p_s^{\alpha_s - 1}(p_s - 1)\phi(d)$$

$\Rightarrow \phi(d)|\phi(n)$

0.3

0.3.1

For $0 \leq k \leq 17$ the residue class $[k]$ of $\mathbb{Z}/18\mathbb{Z}$ is the set $\{k \pm 18n : n \in \mathbb{Z}\}$.

0.3.2

We want to prove that the distinct equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ are precisely $\overline{0}, \overline{1}, ..., \overline{n-1}$. First, note that $\overline{0}, \overline{1}, ..., \overline{n-1}$ partition $\mathbb{Z}$, so indeed they are distinct equivalence classes. Now, let $a \in \mathbb{Z}$. By the division algorithm, $a = nq + r$ for some integers q and r with $0 \leq r \leq n-1$. Thus, $a \equiv r$ (mod n) $\Rightarrow a \in \overline{r}$, which is exactly one of $\overline{0}, \overline{1}, ..., \overline{n-1}$. Therefore, the distinct equivalence classes of $\mathbb{Z}/n\mathbb{Z}$ are $\overline{0}, \overline{1}, ..., \overline{n-1}$

0.3.3

Given that $a = a_n 10^n + a_{n-1}10^{n-1} + ... + a_1 10 + a_0$, we want to show that $a \equiv a_n + a_{n-1} + ... + a_1 + a_0$ (mod 9). Observe that

$$\begin{aligned}
\overline{a} &= \overline{a_n 10^n} + \overline{a_{n-1}10^{n-1}} + ... + \overline{a_1 10} + \overline{a_0} \\
&= \overline{a_n}\,\overline{10}^n + \overline{a_{n-1}}\,\overline{10}^{n-1} + ... + \overline{a_1}\,\overline{10} + \overline{a_0} \\
&= \overline{a_n}\,\overline{1}^n + \overline{a_{n-1}}\,\overline{1}^{n-1} + ... + \overline{a_1}\,\overline{1} + \overline{a_0} \qquad \big(\text{since } 10 \equiv 1 \text{ (mod 9)}\big) \\
&= \overline{a_n} + \overline{a_{n-1}} + ... + \overline{a_1} + \overline{a_0}
\end{aligned}$$

$\Rightarrow a \equiv a_n + a_{n-1} + ... + a_1 + a_0$ (mod 9).

0.3.4

We want 37^{100} (mod 29). First note that $37 \equiv 8$ (mod 29) and $8^{100} = 8^{64}8^{32}8^{4}$; thus, we neet to find 8^{64}, 8^{32}, and 8^{4}, respectively, (mod 29). Observe that:

$$\begin{aligned}
8^2 = 64 &\equiv 6 \text{ (mod 29)} \\
8^4 = (8^2)^2 &\equiv 6^2 \text{ (mod 29)} \\
&\equiv 7 \text{(mod 29)} \\
\\
8^8 = (8^4)^2 &\equiv 7^2 \text{ (mod 29)} \\
&\equiv 20 \text{ (mod 29)} \\
&\equiv -9 \text{ (mod 29)} \\
\\
8^{16} = (8^8)^2 &\equiv (-9)^2 \text{ (mod 29)} \\
&\equiv 23 \text{ (mod 29)} \\
&\equiv -6 \text{ (mod 29)} \\
\\
8^{32} = (8^{16})^2 &\equiv (-6)^2 \text{ (mod 29)} \\
&\equiv 7 \text{ (mod 29)} \\
\\
8^{64} = (8^{32})^2 &\equiv 7^2 \text{ (mod 29)} \\
&\equiv -9 \text{ (mod 29)} \\
\Rightarrow 37^{100} &\equiv (-9)(7)(7) \text{ (mod 29)} \\
&\equiv (-63)(7) \text{ (mod 29)} \\
&\equiv 24(7) \text{ (mod 29)} \\
&\equiv (-5)(7) \text{ (mod 29)} \\
&\equiv -35 \text{ (mod 29)} \\
&\equiv 23 \text{ (mod 29)}
\end{aligned}$$

That is, the remainder of 37^{100} divided by 29 is 23.

0.3.5

We want to compute the last two digits of 9^{1500}. Note that the remainder after dividing by 100 will give us the last two digits of the number (becasue by the division algorithm, $9^{1500} = xq + r$, where $x, q, r \in \mathbb{Z}$ and $0 \leq r < x$; in this case, $x = 100$ since we are dividing by 100). Recall the binomial formula:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Now,

$$
\begin{aligned}
9^{1,500} = (10-1)^{1,500} &= \sum_{k=0}^{1,500} \binom{1,500}{k} 10^k (-1)^{1,500-k} \\
&= 10^{1,500} - \binom{1,500}{1} 10^{1,499} \cdot 1^1 + \binom{1,500}{2} 10^{1,498} \cdot 1^2 \mp ... - \binom{1,500}{1,499} 10^1 \cdot 1^{1,499} + 1^{1,500} \\
&= 100x - 1,500 \cdot 10 + 1, \text{ where } x = \frac{10^{1,500} \mp ... + \binom{1,500}{1,498} 10^2 \cdot 1^{1,498}}{100} \\
&= 100y + 1, \text{ where } y = x - 150
\end{aligned}
$$

Dividing $9^{1,500}$ by 100, we have $y + \frac{1}{100} = y.01 \Rightarrow 9^{1,500} = y01 \Rightarrow$ the last two digits are: 01.

0.3.6

$\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. Now, $0^2 = 0$, $1^1 = 1$, $2^2 = 4 \equiv 0$ (mod 4), and $3^2 = 9 \equiv 1$ (mod 4); hence, the only squares in $\mathbb{Z}/4\mathbb{Z}$ are $\overline{0}$ and $\overline{1}$.

0.3.7

$a^2 + b^2$ (mod 4) equals either 0, 1, or 2 since from the previous problem we know that a^2 and b^2 are congruent (mod 4) to either 0 or 1. Therefore, $a^2 + b^2$ never elaves a remainder of 3 after being divided by 4.

0.3.8

We want to show that $a^2 + b^2 = 3c^2$ has no nonzero solutions. Assume for the sake of contradiction that there exists a nonzero solution $(a^0, b^0, c^0) \in \mathbb{Z}^3$ to the equation $a^2 + b^2 = 3c^2$. Without loss of generality we may assume that $a^0, b^0, c^0 > 0$ since $(a^0)^2 = |a^0|^2$, $(b^0)^2 = |b^0|^2$, and $(c^0)^2 = |c^0|^2$.

I claim that c^2 must be even. To see this, observe that if c^2 is odd, then by 0.3.6, $c^2 \equiv 1$ (mod 4), which implies that $a^2 + b^2 \equiv 3$ (mod 4); this is impossible by 0.3.7. Thus, c^2 is even, and by 0.3.6, $c^2 \equiv 0$ (mod 4) $\Rightarrow a^2 + b^2 \equiv 0$ (mod 4). Moreover, from 0.3.6, a^2 and b^2 are congruent (mod 4) to either 0 or 1; $a^2 + b^2 \equiv 0$ (mod 4) implies that a^2, $b^2 \equiv 0$ (mod 4) $\Rightarrow a$ and b are even. Now, a, b, and c even implies that a^2, b^2, and c^2 are divisible by 4. Therefore, we may divide both sides of the equation $a^2 + b^2 = 3c^2$ by 4 and obtain a solution to the resulting equation (which is still of the form $a^2 + b^2 = 3c^2$) that is strictly smaller than (a^0, b^0, c^0); namely, $(a^1, b^1, c^1) = (\frac{a^0}{2}, \frac{b^0}{2}, \frac{c^0}{2})$.

Since we assumed nothing about a, b, and c (other than that they are positive), we may repeat this process indefinitely, contradicting the well-ordering princple.

0.3.9

Let z be an odd integer. Then there exists $k \in \mathbb{Z}$ such that $z = 2k+1 \Rightarrow z^2 = (2k+1)^2 = 4k^2+4k+1 = 4k(k+1)+1$. The product of two consecutive integers is even, which implies there exists $m \in \mathbb{Z}$ such that $z^2 = 4(2m) + 1 = 8m + 1 \Rightarrow z^2 \equiv 1$ (mod 8); i.e., z leaves a remainder of 1 after being divided by 8.

0.3.10

We want to show that $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$; i.e., we want to show that $|(\mathbb{Z}/n\mathbb{Z})^\times| = |\{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}|$. Recall that $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \exists\, \overline{a} \in \mathbb{Z}/_{n\mathbb{Z}}$ s.t. $\overline{a} \cdot \overline{c} = \overline{1}\}$. Now, $\gcd(a, n) = 1 \iff \exists\, x, y \in \mathbb{Z}$ such that $ax + ny = 1 \iff ax \equiv 1$ (mod n). If $x < n$, we are done. If not, then $ax \equiv ar$ (mod n), where $r :=$ the remainder after dividing x by n; $r < n$. Thus, $\gcd(a, n) = 1 \iff a$ has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$, or equivalently, $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$.

0.3.11

Given that a and b are relatively prime to n, we want to show that ab is relatively prime to n. a and b relatively prime to n implies that there exists $x, x', y, y' \in \mathbb{Z}$ such that

$$ax + ny = 1 = bx' + ny'$$

$$\Rightarrow (ax + ny)(bx' + ny') = 1$$

$$\iff axbx' + axny' + nybx' + n^2yy' = 1$$

$$\Rightarrow abxx' \equiv 1 \text{ (mod n)}$$

$\therefore \exists\, y \in \mathbb{Z}/_{n\mathbb{Z}}$ such that $(ab)y \equiv 1$ (mod n) $\Rightarrow \gcd(ab, n) = 1$; i.e., ab and n are relatively prime.

0.3.12

We aregiven integers n and a such that $n > 1$, $1 \le a < n$, and $\gcd(a, n) = d > 1$. First we want to show that there exists $b \in \mathbb{Z}$ such that $1 \le b < n$ and $ab \equiv 0$ (mod n). Set $b := \frac{n}{d}$. Then observe that $1 \le \frac{n}{d} < n$ and $ab = kd \cdot \frac{n}{d} = kn \equiv 0$ (mod n), since $a = kd$ for some $k \in \mathbb{Z}$.

Now assume for the sake of contradiction that there exists $c \in \mathbb{Z}$ such that $ac \equiv 1$ (mod n). Then $ac \equiv 1$ (mod n) $\iff abc \equiv b$ (mod n) $\iff 0 \equiv b$ (mod n), which is a contradiction since $0 < b = \frac{n}{d} < n$ (mod n).

0.3.13

By the Euclidean algorithm, $\gcd(a, n) = 1 \Rightarrow \exists\, x, y \in \mathbb{Z}$ such that $ax + ny = 1 \iff ny = 1 - ax \iff ax \equiv 1$ (mod n), hence there exists some $c \in \mathbb{Z}$ such that $ac \equiv 1$ (mod n); namely, $c = x$.

0.3.14

Observe that 0.3.13 implies that $(\mathbb{Z}/n\mathbb{Z})^\times$ is a superset of the set $\{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$, and 0.3.12 implies $(\mathbb{Z}/n\mathbb{Z})^\times$ does not contain any elements in the complement of $\{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$, hence $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$. As an example, consider $(\mathbb{Z}/12\mathbb{Z})^\times$. 1 has multiplicative inverse 1, 5 has multiplicative inverse 5, 7 has multiplicative inverse 7, and 11 has multiplicative inverse 11; only these numbers have multiplicative inverses in $\mathbb{Z}/12\mathbb{Z}$, hence $(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$, and these are precisely the integers relatively prime to 12.

0.3.15

(a)

$$\begin{aligned} 20 &= 1(13) + 7 \\ 13 &= 1(7) + 6 \\ 6 &= 6(1) \end{aligned}$$

$\Rightarrow \gcd(20, 13) = 1$; that is, 20 and 13 are relatively prime.

$$\begin{aligned} 1 &= 7 - 1(6) \\ &= [13 - 1(6)] - 1(6) \\ &= 13 - 2(6) \\ &= 13 - 2[13 - 1(7)] \\ &= 2(7) - 1(13) \\ &= 2[20 - 1(13)] - 1(13) \\ &= 2(20) - 3(13) \end{aligned}$$

$\Rightarrow 2(20) = 1 + 3(13) \Rightarrow 20|[1 + 3(13)] \Rightarrow -3(13) \equiv 1 \text{ (mod 20)} \Rightarrow -3 \equiv 17$ (mod 20) is the multiplicative inverse of 13 in $\mathbb{Z}/_{20\mathbb{Z}}$.

(b)

$$\begin{aligned}
89 &= 1(69) + 20 \\
69 &= 3(20) + 9 \\
20 &= 2(9) + 2 \\
9 &= 4(2) + 1 \\
2 &= 2(1)
\end{aligned}$$

$\Rightarrow \gcd(89, 69) = 1$; that is, 89 and 69 are relatively prime.

$$\begin{aligned}
1 &= 9 - 4(2) \\
&= 9 - 4[20 - 2(9)] \\
&= 9(9) - 4(20) \\
&= 9[69 - 3(20)] - 4(20) \\
&= 9(69) - 31(20) \\
&= 9(69) - 31(89 - 69) \\
&= 40(69) - 31(89)
\end{aligned}$$

$\Rightarrow -31(89) = 1 - 40(69) \Rightarrow 89|[1 - 40(69)] \Rightarrow 40(69) \equiv 1$ (mod 89) $\Rightarrow 40$ is the multiplicative inverse of 69 in $\mathbb{Z}/_{89\mathbb{Z}}$.

Parts (c) and (d) are omitted because they are analogous to (a) and (b)

0.3.16

Omitted.