Solutions to
exercises in Number Theory and Abstract Algebra

Problem 1.1

(a)

$$\begin{aligned}
1870 &= 222 \cdot 8 + 94 \\
222 &= 94 \cdot 2 + 34 \\
94 &= 34 \cdot 2 + 26 \\
34 &= 26 \cdot 1 + 8 \\
26 &= 8 \cdot 3 + 2 \\
8 &= 2 \cdot 4 + 0
\end{aligned}$$

Backwards

$$\begin{aligned}
2 &= 26 - 8 \cdot 3 \\
&= 26 - (34 - 26 \cdot 1) \cdot 3 = 4 \cdot 26 - 34 \cdot 3 \\
&= 4 \cdot (94 - 34 \cdot 2) - 34 \cdot 3 = -11 \cdot 34 + 4 \cdot 94 \\
&= -11(222 - 94 \cdot 2) + 4 \cdot 94 = 26 \cdot 94 + (-11 \cdot 222) \\
&= 26 \cdot (1870 - 222 \cdot 8) - 11 \cdot 222 \\
&= 26 \cdot 1870 - 219 \cdot 222
\end{aligned}$$

Problem 1.2

(a) $\phi(36) = \phi(2^2 \cdot 3^2) = (2^2 - 2)(3^2 - 3) = 12$

(b) $\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$

(c) $36 = 7 \cdot 5 + 1$
$1 = 36 - 7 \cdot 5$
$\Rightarrow 5^{-1} = (-7) \bmod 36 = 29$

Problem 1.3

(a) $143 = 71 \cdot 2 + 1 \Rightarrow 2^{-1} = (-71) \bmod 143 = 72$

(b) $2^{-1} \pmod{11} = 6$
$2^{-1} \pmod{13} = 7$

(c) Gauss's algorithm gives
$n_1 = 11, N_1 = 13 \quad M_1 = 6$
$n_2 = 13, N_2 = 11 \quad M_2 = 11^{-1} \pmod{13} = 6$
$$x^{-1} = \sum_{i=1}^{2} a_i N_i M_i \bmod n = 6 \cdot 13 \cdot 6 + 7 \cdot 11 \cdot 6 \bmod 143 = 72$$

Problem 1.4

$n_1 = 7, N_1 = 221, M_1 = 221^{-1} \bmod 7 = 2$
$n_2 = 13, N_2 = 119, M_2 = 119^{-1} \bmod 13 = 7$
$n_3 = 17, N_3 = 91, M_3 = 91^{-1} \bmod 17 = 3$
$n = n_1 n_2 n_3 = 1547$
$$x = \sum_{i=1}^{3} a_i N_i M_i \bmod n = 3 \cdot 221 \cdot 2 + 1 \cdot 119 \cdot 7 + 13 \cdot 91 \cdot 3 = 1067$$
The integer solutions are $1067 + k \cdot 1547$, where $k \in \mathbb{Z}$.

Problem 1.5

Removed.

Problem 1.6

(a) $2/5 = 2 \cdot 5^{-1} = 2 \cdot 5 = 2$ in $\mathbb{Z}_8$ since $5^{-1} = 5$.

(b) $5^2 = 1 \Rightarrow \text{ord}(5) = 2$

(c) $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. It is cyclic if there is an element of order 4. But $\text{ord}(3) = 2$ and $\text{ord}(7) = 2$, so $\mathbb{Z}_8^*$ is not cyclic.

Problem 1.7

Find x s.t $x^2 = 10$. By testing we find $6^2 = 36 \bmod 13 = 10$.
So $\sqrt{10} = 6$ in $\mathbb{Z}_{13}$.

Problem 1.8

(a) The defined addition is associative, $(0, 0, 0)$ is the identity element, and every element has additive inverse, namely itself.

(b) 8

(c) 2

(d) No, since all elements are its own inverse, there is no element of order 8.

Problem 1.9

The element 1 is a generator, since the set $\{1, 1 + 1, 1 + 1 + 1, \ldots\}$ contains all elements in $\mathbb{Z}_{13}$.

Problem 1.10

The element 2 is a generator of $\mathbb{Z}_{19}^*$ (since $2^2 \neq 1, 2^9 \neq 1$). Since $\phi(19) = 18$, there is one subgroup of order 2, one of order 3, one of order 6, and one of order 9.

They are

$\{2^9, 2^{18} = 1\}$

$\{2^6, 2^{12}, 2^{18} = 1\}$

$\{2^3, 2^6, 2^9, 2^{12}, 2^{15}, 2^{18} = 1\}$

$\{2^2, 2^4, 2^6, 2^8, 2^{10}, 2^{12}, 2^{14}, 2^{16}, 2^{18} = 1\}$

Then there are also the trivial subgroups $\{1\}$ and $\mathbb{Z}_{19}^*$.

(If $G =< g >$ is a finite cyclic group of order n, then any subgroup of G has the form $H =< g^d >$ for a divisor $d|n$. Different values of d give different sizes so there is just one subgroup of G having a given size.)

Problem 1.11

Since the element 2 has no multiplicative inverse, $\mathbb{Z}_4$ is no field.

Problem 1.12

$F : \alpha^3 + \alpha + 1 = 0$ $\qquad\qquad$ $F' : \beta^3 + \beta^2 + 1 = 0$

1	1
α	β
α^2	β^2
$\alpha^3 = \alpha + 1$	$\beta^3 = \beta^2 + 1$
$\alpha^4 = \alpha^2 + \alpha$	$\beta^4 = \beta^2 + \beta + 1$
$\alpha^5 = \alpha^2 + \alpha + 1$	$\beta^5 = \beta + 1$
$\alpha^6 = \alpha^2 + 1$	$\beta^6 = \beta^2 + \beta$
$\alpha^7 = 1$	$\beta^7 = 1$

We see that $\gamma(1) = 1$. Now let $\gamma(\alpha) = x$. We write

$$\begin{aligned} \gamma(\alpha^3) &= \gamma(\alpha)\gamma(\alpha)\gamma(\alpha) = x^3 \\ &= \gamma(\alpha + 1) = \gamma(\alpha) + 1 = x + 1 \end{aligned}$$

This implies $x^3 + x + 1 = 0$, where $x \in F'$.
By testing we find $x = \beta^3$. Thus

$$\begin{cases} \gamma(1) &= 1 \\ \gamma(\alpha) &= \beta^2 + 1 \\ \gamma(\alpha^2) &= \beta^2 + \beta \end{cases}$$

Problem 1.13

(a) $\alpha + 1$

(b) α

(c) α^3

(d) $x = \alpha^2$

Problem 1.14

(a) primitive (and irreducible)

(b) irreducible

(c) reducible $x^4 + x^2 + 1 = (x^2 + x + 1)^2$

(d) reducible, since $x^4 + x + 1 = 0$ if $x = 1$.