Solutions to Homework Set 2
(Homework Problems from Chapter 1)

Problems from Section 1.1.

1.1.1
Let n be an integer. Prove that a and c leave the same remainder when divided by n if and only if $a-c=nk$ for some $k \in \mathbb{Z}$.

Proof.

$\Rightarrow$
Suppose $a-c=nk$. By the division algorithm, there exist unique integers q_1, r_1, q_2, r_2 such that

$$\begin{aligned} a &= nq_1 + r_1 \quad ; \quad 0 \leq r_1 < n \\ c &= nq_2 + r_2 \quad ; \quad 0 \leq r_2 < n \quad . \end{aligned}$$

But then we have

$$\begin{aligned} a-c &= nk+0 \\ a-c &= n(q_1-q_2)+(r_1-r_2) \end{aligned}$$

Thus

$$r_1 - r_2 = n(q_1 - q_2 + k)$$

and so $r_1 - r_2$ is divisible by n. However, the conditions $0 \leq r_1, r_2 < n$ imply

$$0 \leq |r_1 - r_2| < n$$

But the only non-negative integer divisible by n and less than n is 0. Hence, $r_1 - r_2 = 0$, or $r_1 = r_2$.

$\Leftarrow$
Assume $a = nq_1 + r$ and $c = nq_2 + r$. Then $a - c = n(q_1 - q_2)$. So $a - c$ is divisible by n. ∎

1.1.2
Let a and b be integers with $c \neq 0$. Then there exist unique integers q and r such that

$$\begin{aligned} (i) &\quad a = cq + r \\ (ii) &\quad 0 \leq r < |c| \quad . \end{aligned}$$

Proof.

If c is positive, then $c = |c|$ and this is just the statement of the Division Algorithm (Theorem 1.1) so there is nothing more to prove.

If c is negative, then $-c = |c|$ is positive and we can apply the Division Algorithm: there exist unique integers q' and r' such that

$$a = |c|q' + r' \quad \text{and} \quad 0 \leq r' < |c| \quad ,$$

or, equivalently

$$a = -cq' + r' \quad \text{and} \quad 0 \leq r' < |c| \quad .$$

We have thus shown that there exist integers q and r satisfying (i). We must now show this choice of q and r is unique. Suppose we have $q, r, q', r' \in \mathbb{Z}$ such that

$$\begin{array}{ccc} a = cq + r & ; & 0 \leq r < |c| \\ a = cq' + r' & ; & 0 \leq r' < |c| \end{array}$$

Then we have

$$0 = c(q - q') + r - r'$$

or

$$(\star) \qquad r - r' = c(q' - q) \quad .$$

So $r - r'$ is divisible by c. But also $|r - r'| < |c|$. Hence, since 0 is the only non-negative number less than $|c|$ that is divisible by c, we must have $r - r' = 0$. But this with $(\star)$ then implies $q - q' = 0$. Hence, $q = q'$ and $r = r'$. So q and r are unique. ∎

1.1.3
Prove that the square of any integer a is either of the form $3k$ or of the form $3k + 1$ for some integer k.

Proof.

By the Division Algorithm, any integer a is representable as

$$a = 3q + r$$

with r an integer such that $0 \leq r < 3$. That means $r \in \{0, 1, 2\}$. So a has one of three possible forms

$$(1) \qquad a = 3q + 0$$

$$(2) \qquad a = 3q + 1$$

$$(3) \qquad a = 3q + 2$$

In the first case, $a^2 = 9q^2 = 3(3q^2)$ is obviously of the form $3k$, with $k = 3q^2$. In the second case,

$$\begin{aligned} a^2 &= (3q + 1)^2 \\ &= 9q^2 + 6q + 1 \\ &= 3(3q^2 + 2q) + 1 \end{aligned}$$

and so a^2 is of the form $3k + 1$, with $k = 3q^2 + 2q$. In the last case,

$$\begin{aligned} a^2 &= (3q + 2)^2 \\ &= 9q^2 + 12q + 4 \\ &= 3(3q^2 + 4q + 1) + 1 \end{aligned}$$

a^2 is also of the form $3k + 1$, with $k = 3q^2 + 4q + 1$. ∎

1.1.4
Prove that the cube of any integer has exactly one of the forms $9k$, $9k + 1$, or $9k + 8$.

Let a be any integer. Then by the Division Algorithm, a must have one of the following forms

$$a = \left\{ \begin{array}{c} 3q \\ 3q + 1 \\ 3q + 2 \end{array} \right. .$$

So

$$a^3 = \left\{ \begin{array}{c} 27q^3 = 9(3q^3) \\ 27q^3 + 18q^2 + 18q + 1 = 9(3q^3 + 2q^2 + 2q) + 1 \\ 27q^3 + 36q^2 + 72q + 8 = 9(3q^3 + 4q^2 + 8q) + 8 \end{array} \right.$$

Problems from Section 1.2

1.2.1

(a) Prove that if $a \mid b$ and $a \mid c$ then $a \mid (b+c)$.

Proof.
If $a \mid b$ and $a \mid c$, then there exist integers q_1 and q_2 such that

$$\begin{aligned} b &= q_1 a \\ c &= q_2 a \end{aligned}$$

So

$$b + c = q_1 a + q_2 a = a(q_1 + q_2) \quad .$$

So $b+c$ is divisible by a. ∎

(b) Prove that if $a \mid b$ and $a \mid c$, then $a \mid (br + ct)$ for any $r, t \in \mathbb{Z}$.

Proof.

Again we have

$$\begin{aligned} b &= q_1 a \\ c &= q_2 a \end{aligned}$$

and so

$$\begin{aligned} br + ct &= (q_1 a) r + (q_2 a) t \\ &= a(q_1 r + q_2 t) \quad . \end{aligned}$$

Hence $br + ct$ is divisible by a. ∎

1.2.2
Prove or disprove that if $a \mid (b+c)$, then $a \mid b$ or $a \mid c$.

Disproof by counter-example.

Take $a = 6$, $b = c = 3$. Then $6 \mid (3+3)$ but $6 \nmid 3$. ∎

1.2.3
Prove that if $r \in \mathbb{Z}$ is a non-zero solution of $x^2 + ax + b = 0$ (where $a, b \in \mathbb{Z}$), then $r \mid b$.

Proof.

By hypothesis,

$$r^2 + ar + b = 0$$

or

$$b = r(-r - a) \quad .$$

It is thus clear that r divides b if r is nonzero. ∎

1.2.4
Prove that $GCD(a, a+b) = d$ if and only if $GCD(a, b) = d$.

Proof.

Let

$$\begin{aligned} S &= \{\text{common divisors of} a \text{ and} b\} \\ T &= \{\text{common divisors of} a \text{ and} (a+b)\} \end{aligned}$$

We will show that these two sets coincide.

Suppose $s \in S$. Then there exist $x, y \in \mathbb{Z}$ such that

$$\begin{aligned} a &= xs \\ b &= ys \end{aligned}$$

Thus,

$$a + b = sx + sy = s(x+y) \quad ,$$

and so $a + b$ is divisible by s. So any $s \in S$ is also an element of T.

Suppose $t \in T$. Then there exist $u, v \in \mathbb{Z}$ such that

$$\begin{aligned} a &= ut \\ a+b &= vt \quad . \end{aligned}$$

Hence,

$$b = vt - ut = t(v-u) \quad ,$$

and so b is also divisible by t. So any element $t \in T$ is also an element of S.

Thus, $S = T$. So

$$GCD(a,b) = \text{Max}(S) = \text{Max}(T) = GCD(a, a+b) \quad .$$

∎

1.2.5
Prove that if $GCD(a,c) = 1$ and $GCD(b,c) = 1$, then $GCD(ab,c) = 1$.

Proof.

Suppose $GCD(a,c) = 1$ and $GCD(b,c) = 1$. Then by Theorem 1.3, there exists integers u, v, x, y such that

$$\begin{aligned} 1 &= ua + vc \\ 1 &= xb + yc \end{aligned}$$

But then

$$\begin{aligned} 1 &= 1 \cdot 1 \\ &= (ua + vc)(xb + yc) \\ &= (ux)\, ab + (uay + vxb + vyc)\, c \end{aligned}$$

Thus,

$$1 = u'(ab) + v'c \tag{4}$$

with

$$\begin{aligned} u' &= ux \\ v' &= uay + vxb + vyc \quad . \end{aligned}$$

Now let t be any common divisor of ab and c. Then, by definition, there exists $s, t \in \mathbb{Z}$ such that

$$\begin{aligned} ab &= rt \\ c &= st \end{aligned}$$

So we can rewrite (4) as

$$1 = u'rt + v'st = (u'r + v's)\,t \quad ;$$

from which it is clear that $t \mid 1$. Hence, $t = \pm 1$. Hence the greatest common divisor of ab and c is 1. ∎

* * * * * * **

Here is an alternative proof.

First of all, it is clear that if c and b have no common factors, and t is a factor of b, then c and t have no common factors. Put another way; if $t \mid c$ and $GCD(c,b) = 1$ then $GCD(t,b) = 1$.

Now suppose that $d = GCD(c, ab)$. Then $d \geq 1$ and there exist integers x and y such that

$$\begin{aligned} c &= xd \\ ab &= yd \quad . \end{aligned}$$

Since $d \mid c$ and $GCD(a,c) = 1$, by the remark above above, we have $GCD(t,a) = 1$.

Similarly, t divides c and $GCD(b,c) = 1$ implies $GCD(t,b) = 1$.

Now we apply Theorem 1.5.

$$t \mid ab \quad \text{and} \quad GCD(t,a) = 1 \quad \Rightarrow \quad t \mid b.$$

But $GCD(t,b) = 1$. Hence $t = 1$. ∎

1.2.6
(a) Prove that if $a, b, u, v \in \mathbb{Z}$ are such that $au + bv = 1$, then $GCD(a,b) = 1$.

Proof.

First note that the condition $au + bv = 1$ implies that a and b cannot both be zero. According to Corollary 1.4, an integer d is the greatest common divisor of a and b if and only if

(i) $d \mid a$ and $d \mid b$
(ii) if $c \mid a$ and $c \mid b$, then $c \mid d$.

Suppose now that $d = GCD(a,b) > 1$. Then

$$\begin{aligned} a &= sd \\ b &= td \quad . \end{aligned}$$

But then we have

$$1 = sdu + tdv = d(su + tv)$$

But now note that the right hand side is divisible by d but the left hand side is not, since d is presummed to be greater than 1. Hence we have a contradiction unless $d = 1$. ∎

(b) Show by example that if $au + bv = d > 0$, then $GCD(a,b)$ need not be d.

Example.

Take $a = 3$, $u = 1$, $b = 3$, $v = 1$. Then

$$au + bv = 5$$

but

$$GCD(3,2) = 1 \quad .$$

∎

Problems from Section 1.3

1.3.1
Let p be an integer other than $0, \pm 1$. Prove that p is prime if and only if for each $a \in \mathbb{Z}$, either $GCD(a,p) = 1$ or $p \mid a$.

Proof.
$\Rightarrow$

If p is prime then the only divisors of p are ± 1 and $\pm p$. So if s is a common divisor of a and p, then $s \in \{\pm 1, \pm p\}$. Hence either $GCD(a,p) = 1$ or $GCD(a,p) = |p|$. In the latter case we have $p \mid a$. So either $GCD(a,p) = 1$ or $p \mid a$. ∎

$\Leftarrow$ (Proof by Contradiction)

Assume p has the property that for every integer a, either $GCD(a,p) = 1$ or $p \mid a$. If p is not prime then there exist $s, t \in \mathbb{Z}$ such that

$$p = st$$

and

$$1 < |s| \leq |t| < |p| \quad .$$

Since t is a divisor of p, $GCD(t,p) = t \neq 1$. Therefore, $p \mid t$. But this is impossible since $|t| < |p|$. Hence p must be prime.

1.3.2
Let p be an integer other than 0 ± 1 with this property: Whenever b and c are integers such that $p \mid bc$, then $p \mid c$ or $p \mid b$. Prove that p is prime.

Proof.

Suppose p is an integer $\neq 0, \pm 1$ such that whenever $p \mid bc$ then $p \mid b$ or $p \mid c$. Let s be a divisor of p. Then $p = sq$ for some integer q and we have

$$sq \mid bc \quad \Rightarrow \quad sq \mid b \quad \text{or} \quad sq \mid c$$

In particular, taking $b = s$ and $c = q$, we have

$$sq \mid s \quad \text{or} \quad sq \mid q \quad .$$

But this implies either

$$s = \pm 1 \quad \text{and} \quad q = \pm p$$

or

$$s = \pm p \quad \text{and} \quad q = \pm 1 \quad .$$

Hence the only divisors of p are ± 1 and $\pm p$; and so p is prime. ∎

1.3.3
Prove that if every integer integer $n > 1$ can be written in one and only one way in the form

$$n = p_1 p_2 \cdots p_r$$

where the p_i are positive primes such that $p_1 \leq p_2 \leq \cdots \leq p_r$.

Proof.

By Theorem 1.11, we know that there exists a prime factorization of n that is unique up to changes in the order of factors and flips in the sign of pairs of factors. The statement above just removes the remaining ambiguity in the conclusion of Theorem 1.11. All prime factors are now required to be positive, so there one cannot flip the sign of terms; and the order of factors is fixed to coincide with their normal ordering as integers. ∎

1.3.4
Prove that if p is prime and $p \mid a^n$, then $p^n \mid a^n$.

Proof.

According to Corollary 1.9, if $p \mid a^n$, then $p \mid a$ since $a^n = a \cdot a \cdot a \cdot \cdots \cdot a$. But then $a = pq$ for some $q \in \mathbb{Z}$. Hence $a^n = p^n q^n$, and so p^n divides a^n. ∎

1.3.5
(a) Prove that there exist no nonzero integers a, b such that $a^2 = 2b^2$.

Proof.

According to the Fundamental Theorem of Arithmetic, a and b have prime factorizations of the form

$$\begin{aligned} a &= p_1 p_2 \cdots p_r \\ b &= q_1 q_2 \cdots q_s \quad . \end{aligned}$$

But then

$$\begin{aligned} a^2 &= p_1 p_1 p_2 p_2 \cdots p_r p_r && (2r \text{ prime factors}) \\ 2b^2 &= 2 q_1 q_1 q_2 q_2 \cdots q_s q_s && (2s+1 \text{ prime factors}) \end{aligned}$$

Since the two integers a^2 and $2b^2$ have, respectively, an even number and an odd number of prime factors, a^2 can not equal $2b^2$. ∎

(b) Prove that $\sqrt{2}$ is irrational.

Proof.

Suppose $\sqrt{2}$ is rational; i.e., $\sqrt{2} = \frac{a}{b}$ with $a, b \in \mathbb{Z}$, $b \neq 0$. Then

$$\sqrt{2} b = a$$

is an integer. Squaring both sides of this equation we get

$$2b^2 = a^2$$

which as we have just seen cannot be satified by any non-zero integers a and b. Hence we have a contradiction. So $\sqrt{2}$ can not be rational. ∎