SOLUTIONS TO PROBLEM SET 1

Section 1.3

Exercise 4. We see that

$$\frac{1}{1\cdot 2} = \frac{1}{2}, \qquad \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} = \frac{2}{3}, \qquad \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} = \frac{3}{4},$$

and is reasonable to conjecture

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}.$$

We will prove this formula by induction.

Base $n=1$: It is shown above.

Hypothesis: Suppose the formula holds for n.

Step:

$$\begin{aligned}
\sum_{k=1}^{n+1} \frac{1}{k(k+1)} &= \sum_{k=1}^{n} \frac{1}{k(k+1)} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n(n+2)+1}{(n+1)(n+2)} = \frac{n^2+2n+1}{(n+1)(n+2)} \\
&= \frac{(n+1)^2}{(n+1)(n+2)} = \frac{n+1}{n+2},
\end{aligned}$$

where in the second equality we used the induction hypothesis.

Exercise 14. We will use strong induction.

Base $54 \le n \le 60$: We have

$$54 = 7\cdot 2 + 10\cdot 4, \quad 55 = 7\cdot 5 + 10\cdot 2, \quad 56 = 7\cdot 8 + 10\cdot 0, \quad 57 = 7\cdot 1 + 10\cdot 5$$

and

$$58 = 7\cdot 4 + 10\cdot 3, \quad 59 = 7\cdot 7 + 10\cdot 1, \quad 60 = 7\cdot 0 + 10\cdot 6.$$

Hypothesis: Suppose the result holds for $54 \le k \le n$.

Step $n \ge 60$: We have $n-6 \ge 54$, hence by the induction hypothesis we can write

$$n - 6 = 7a + 10b \quad \text{for some } a, b \in \mathbb{Z}_{>0}.$$

Then $n+1 = 7(a+1) + 10b$, as desired.

Exercise 22. We will use induction.

Base $n = 0$*:* We have $1 + 0h = 1 = (1+h)^0$, as desired.

Hypothesis: Suppose the result holds for n.

Step $n \geq 0$: We have

$$\begin{aligned}(1+h)^{n+1} &= (1+h)^n(1+h)\\ &\geq (1+nh)(1+h)\\ &= 1+h+nh+nh^2\\ &\geq 1+(n+1)h,\end{aligned}$$

where in the first inequality we used the induction hypothesis and $1 + h \geq 0$.

Exercise 24. The proof fails in the statement that the sets $\{1, \dots, n\}$ and $\{2, \dots, n+1\}$ have common members. This is false when $n = 1$; indeed, the sets are $\{1\}$ and $\{2\}$ which are clearly disjoint.

Section 1.5

Exercise 26. Let $a, b \in \mathbb{Z}_{>0}$.

We first prove **existence**. The division algorithm gives $q', r' \in \mathbb{Z}$ such that

$$a = bq' + r' \quad \text{with} \quad 0 \leq r' < b.$$

We now divide into two cases:

(i) Suppose $r' \leq b/2$; then $-b/2 < r' \leq b/2$. The result follows by taking $q = q'$ and $r = r'$.

(ii) Suppose $b/2 < r' < b$; then $-b/2 < r' - b < 0$. We have

$$a = bq' + r' = bq' + b + r' - b = b(q'+1) + (r'-b),$$

Write $q = q' + 1$ and $r = r' - b$. Then

$$a = bq + r, \quad \text{with} \quad -b/2 < r < 0 \leq b/2.$$

as desired.

We now prove **uniqueness**. Suppose

$$a = bq_1 + r_1 = bq_2 + r_2, \quad \text{with} \quad -b/2 < r_1, r_2 \leq b/2.$$

Then $b(q_1 - q_2) = (r_2 - r_1)$ and b divides $r_2 - r_1$. Since $-b < r_2 - r_1 < b$ it follows that $r_2 - r_1 = 0$ because there is no other multiple of b in this interval. We conclude that $r_1 = r_2$ and $b(q_1 - q_2) = 0$; thus we also have $q_1 = q_2$, as desired.

Exercise 36. Let $a \in \mathbb{Z}$. Dividing a by 3 we get $a = 3q + r$ with $r = 0, 1, 2$. Note that

$$a^3 - a = (a-1)a(a+1) = (3q+r-1)(3q+r)(3q+r+1)$$

and clearly for any choice of $r = 0, 1, 2$ one of the three factors is a multiple of 3. This is the same as saying that in among three consecutive integers one must be a multiple of 3.

Exercise 12. Let $a \in \mathbb{Z}_{>0}$.

We first prove **existence**. We will use strong induction.

Base $a \le 2$. If $a = 1$ take $k = 0$ and $e_0 = 1$; if $a = 2$ take $k = 1$, $e_1 = 1$ and $e_0 = -1$.

Hypothesis: Suppose the desired expression exists for all positive integers $< a$.

Step $a \ge 3$. From the modified division algorithm (Problem 26 in Section 1.5) there exist $q, e_0 \in \mathbb{Z}$ such that

$$a = 3q + r, \quad \text{with} \quad -3/2 < r \le 3/2;$$

in particular, $r = -1, 0, 1$. We have $0 < q = (a - r)/3 < a$ and by hypothesis we can write

$$q = a_s 3^s + \ldots + a_1 3 + a_0, \quad a_s \neq 0, \quad a_i \in \{-1, 0, 1\}.$$

Thus we have

$$a = 3q + r = 3(a_s 3^s + \ldots + a_1 3 + a_0) + r = a_s 3^{s+1} + \ldots + a_1 3^2 + a_0 3 + r$$

and we take $k = s + 1$, $e_0 = r$ and $e_i = a_{s-1}$ for $i = 1, .., k$.

We now prove **uniqueness**. We will use strong induction. Suppose

$$a = e_k 3^k + \ldots + e_1 3 + e_0 = c_s 3^s + \ldots + c_1 3 + c_0, \quad e_k, a_s \neq 0, \quad e_i, a_i \in \{-1, 0, 1\}.$$

Base $a \le 2$*:* We know from above that if $a = 1$ can we take $k = 0$ and $e_0 = 1$ and if $a = 2$ we can take $k = 1$, $e_1 = 1$ and $e_0 = -1$, as balanced ternary expansions. Note also that 0 cannot be written as an expansion using non-zero coefficients.

Suppose now $a = 1 = e_k 3^k + \ldots + e_1 3 + e_0$ with $k \ge 1$; then a divided by 3 has reminder $e_0 = 1$ by the division algorithm. We conclude that $e_k 3^k + \ldots + e_1 3 = 0$ which is impossible, unless $e_i = 0$ for all $i \ge 1$.

Suppose $a = 2 = 1 \cdot 3 - 1 = e_k 3^k + \ldots + e_1 3 + e_0$ with $k \ge 1$; then a divided by 3 has reminder $e_0 = -1$ by the modified division algorithm. We conclude that $e_k 3^k + \ldots + e_1 3 = 3$. Dividing both sides by 3 we conclude that $e_k 3^{k-1} + \ldots + e_1 = 1$ which gives $k = 1$ and $e_1 = 1$ by the previous paragraph. This shows that $a = 1, 2$ have an unique balanced ternary expansion.

Hypothesis: Suppose the expansion is unique for all positive integers $< a$.

Step $a \ge 3$*:* By the uniqueness of the modified division algorithm (Problem 26, Section 1.5), dividing a by 3 we conclude $e_0 = c_0$. Now

$$\frac{a - e_0}{3} = e_k 3^{k-1} + \ldots + e_1 = c_s 3^{s-1} + \ldots + c_1$$

and by induction hypothesis we have $k = s$ and $e_i = c_i$ for $i = 1, .., k$.

Finally, suppose $a < 0$; we apply the result to $-a > 0$ and (due to the symmetry of the coefficients) we obtain the expansion for a by multiplying by -1 the expansion for $-a$.

Exercise 13. Let w be the weight to be measured. From the previous exercise we can write

$$w = e_k 3^k + \ldots + e_1 3 + e_0, \quad e_k \neq 0, \quad e_i \in \{-1, 0, 1\}.$$

Place the object in pan 1. If $e_i = 1$, then place a weight of 3^i into pan 2; if $e_i = -1$, then place a weight of 3^i into pan 1; if $e_i = 0$ do nothing; in the end the pans are balanced.

Exercise 17. Let $n \in \mathbb{Z}_{>0}$ be given in base b by

$$n = a_k b^k + \ldots + a_1 b + a_0, \quad a_k \neq 0, \quad 0 \leq a_i < b.$$

Let $m \in \mathbb{Z}_{>0}$. We want to find the base b expansion of $b^m n$, that is

$$b^m n = c_s b^s + \ldots + c_1 b + c_0, \quad c_s \neq 0, \quad 0 \leq c_i < b.$$

Multiplying both sides of the first equation by b^m gives

$$b^m n = a_k b^{k+m} + \ldots + a_1 b^{m+1} + a_0 b^m, \quad a_k \neq 0, \quad 0 \leq a_i < b.$$

We know that the expansion in base b is unique, so by comparing the last two equations we conclude that

$$s = k + m, \quad c_{s-i} = a_{k-i} \text{ for } i = 0, \ldots, k \quad \text{and} \quad c_i = 0 \text{ for } i = 0, \ldots, m-1,$$

which means

$$b^m n = (c_s c_{s-1} \ldots c_0)_b = (a_k a_{k-1} \ldots a_1 a_0 00 \ldots 0)_b,$$

where we have m zeros in the end.

Section 3.1

Exercise 6. Let $n \in \mathbb{Z}$. Note the factorization $n^3 + 1 = (n+1)(n^2 - n + 1)$ into two integers. If $n^3 + 1$ is a prime, then $n \geq 1$ and $n + 1$ is either 1 or prime. Since $n + 1 \neq 1$ we have $n + 1$ is prime and hence $n^2 - n + 1$ must be 1, which implies $n = 0, 1$. We conclude $n = 1$, as desired.

Exercise 8. Let $n \in \mathbb{Z}_{>0}$. Consider $Q_n = n! + 1$. There is a prime factor $p \mid Q_n$. Suppose $p \leq n$; then $p \mid n! = n(n-1)(n-2)\cdots 2 \cdot 1$ therefore $p \mid Q_n - n! = 1$, a contradiction. We conclude that $p > n$. In particular, given a positive integer n we can always find a prime larger than n; by growing n we produce infinitely many arbitrarily large primes.

Exercise 9. Note that if $n \leq 2$, then $S_n \leq 1$. Therefore, we must assume that $n \geq 3$ so that $S_n > 1$. It follows then that S_n has a prime divisor p. If $p \leq n$, then $p \mid n!$, and so $p \mid (n! - S_n) = 1$, a contradiction. Thus $p > n$. Because we can find arbitrarily large primes, there must be infinitely many.

Section 3.3

Exercise 6. Let $a \in \mathbb{Z}_{>0}$ and write $d = (a, a+2)$. In particular, d divides both a and $a + 2$, hence d also divides the difference $(a+2) - a = 2$. We conclude $d = 1$ or $d = 2$. Now, if a is odd then $a + 2$ is also odd, hence $d = 1$; if a is even then 2 divides both a and $a + 2$, so $d = 2$. We conclude that $(a, a+2) = 1$ if and only if a is odd and $(a, a+2) = 2$ if and only if a is even.

Exercise 10. Write $d = (a+b, a-b)$. If $d = 1$ there is nothing to prove. Suppose $d \neq 1$ and let p be a prime divisor of d (which exists because $d \neq 1$). In particular, p is a common divisor of $a + b$ and $a - b$, therefore it divides both their sum and difference; more precisely, p divides

$$(a+b) + (a-b) = 2a \qquad \text{and} \qquad (a+b) - (a-b) = 2b.$$

Furthermore, since p is prime we also have

(i) $p \mid 2a$ implies $p = 2$ or $p \mid a$,

(ii) $p \mid 2b$ implies $p = 2$ or $p \mid b$.

Suppose $p \neq 2$. Then in (i) we have $p \mid a$ and in (ii) we have $p \mid b$; this is a contradiction with $(a, b) = 1$. We conclude that $p = 2$.

So far we have shown that the unique prime factor of d is 2, therefore $d = 2^k$ with $k \geq 1$. To finish the proof we need to prove that $k = 1$. Since $d \mid a + b$ and $d \mid a - b$ arguing as above we conclude that $2^k \mid 2a$ and $2^k \mid 2b$, that is

$$2a = 2^k x \quad \text{and} \quad 2b = 2^k y \quad \text{for some } x, y \in \mathbb{Z}.$$

Suppose $k \geq 2$. Then dividing both equations by 2 we get

$$a = 2^{k-1} x \quad \text{and} \quad b = 2^{k-1} y$$

with $k - 1 \geq 1$. In particular $2 \mid a$ and $2 \mid b$, a contradiction with $(a, b) = 1$, showing that $k = 1$, as desired.

Here is an alternative, shorter proof using one of the main theorms on gcd:

Let $a, b \in \mathbb{Z}$ satisfy $(a, b) = 1$. There exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Then

$$(a + b)(x + y) + (a - b)(x - y) = 2ax + 2by = 2(ax + by) = 2$$

and since $(a + b, a - b)$ is the smallest positive integer that can be written as an integral linear combination of $a + b$ and $a - b$ we must have $(a + b, a - b) \leq 2$. Thus $(a + b, a - b) = 1, 2$ as desired.

Exercise 12. Let $a, b \in \mathbb{Z}$ be even and not both zero. There exist $x, y \in \mathbb{Z}$ such that

$$ax + by = (a, b) \Leftrightarrow \frac{a}{2}x + \frac{b}{2}y = \frac{(a, b)}{2}.$$

Since $(a/2, b/2)$ is the smallest positive integer that can be written as an integral linear combination of $a/2$ and $b/2$ we must have $(a/2, b/2) \leq (a, b)/2$.

To finish the proof we will show that $(a/2, b/2) \geq (a, b)/2$. There exist $x, y \in \mathbb{Z}$ such that

$$\frac{a}{2}x + \frac{b}{2}y = (a/2, b/2) \Leftrightarrow ax + by = 2(a/2, b/2).$$

Since (a, b) is the smallest positive integer that can be written as an integral linear combination of a and b we conclude $(a/2, b/2) \geq (a, b)/2$, as desired.

Exercise 24. Let $k \in \mathbb{Z}_{>0}$. Suppose d is a common divisor of $3k + 2$ and $5k + 3$. Then d divides every integral linear combination of these numbers. In particular, d divides

$$5(3k + 2) - 3(5k + 3) = 15k + 10 - 15k - 9 = 1,$$

hence $(3k + 2, 5k + 3) = 1$, as desired.

Section 3.4

Exercise 2. We will use the Euclidean algorithm.

a) Compute $(51,87)$**.**

$$87 = 51 \cdot 1 + 36, \quad 51 = 36 \cdot 1 + 15, \quad 36 = 15 \cdot 2 + 6, \quad 15 = 6 \cdot 2 + 3, \quad 6 = 3 \cdot 2 + 0,$$

thus $(51,87) = 3$.

b) Compute $(105,300)$**.**

$$300 = 105 \cdot 2 + 90, \quad 105 = 90 \cdot 1 + 15, \quad 90 = 15 \cdot 6 + 0,$$

thus $(105,300) = 15$.

c) Compute $(981,1234)$**.**

$$1234 = 981 \cdot 1 + 253, \quad 981 = 253 \cdot 3 + 222, \quad 253 = 222 \cdot 1 + 31$$

and

$$222 = 31 \cdot 7 + 5, \quad 31 = 5 \cdot 6 + 1, \quad 5 = 1 \cdot 5 + 0,$$

thus $(981,1234) = 1$.

Exercise 6.

a) Compute $(15,35,90)$**.**

Note that $90 = 15 \cdot 6$ then $((15,90),35) = (15,35) = 5$.

b) Compute $(300,2160,5040)$**.**

Note that $1260 = 300 \cdot 7 + 60$ and $300 = 60 \cdot 5$ thus $(300,2160) = 60$.

Since $5040 = 60 \cdot 84$ we also have

$$(300,2160,5040) = ((300,2160),5040) = (60,5040) = 60.$$

Section 3.5

Exercise 10. Let $a,b \in \mathbb{Z}_{>0}$. Suppose $a^3 \mid b^2$.

Write $a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ for the prime factorization of a. Write $p_i^{b_i}$ for the largest power of p_i diving b. In particular, we can write $b = p_i^{b_i} \cdot m$ for some $m \in \mathbb{Z}$, with $p_i \nmid m$.

From $a^3 \mid b^2$ it follows that $p_i^{3a_i} \mid p_i^{2b_i} m^2$ and since $p_i \nmid m$ we must have $p_i^{3a_i} \mid p_i^{2b_i}$. This implies $2b_i - 3a_i \geq 0$, hence $b_i/a_i \geq 3/2 > 1$. Thus $b_i > a_i$ for all i. Hence we can write

$$b = p_1^{a_1} p_1^{b_1 - a_1} \cdot p_2^{a_2} p_2^{b_2 - a_2} \cdot \dots \cdot p_k^{a_k} p_k^{b_k - a_k} \cdot m'$$

for some $m' \in \mathbb{Z}$ (note that m' is needed since b may have prime factors which are none of the p_i). Therefore, by reordering the factors we also have

$$b = (p_1^{a_1} p_2^{a_2} \dots p_k^{a_k})(p_1^{b_1 - a_1} p_2^{b_2 - a_2} \cdot \dots \cdot p_k^{b_k - a_k}) \cdot m' = a(p_1^{b_1 - a_1} p_2^{b_2 - a_2} \cdot \dots \cdot p_k^{b_k - a_k}) \cdot m'.$$

Thus $a \mid b$, as desired.

Exercise 30. We will use the formulas for (a,b) and $\mathrm{LCM}(a,b)$ in terms of the prime factorizations of a and b.

a) $a = 2\cdot 3^2\cdot 5^3$, $b = 2^2\cdot 3^3\cdot 7^2$. Thus
$$(a,b) = 2\cdot 3^2, \qquad \mathrm{LCM}(a,b) = 2^2\cdot 3^3\cdot 5^3\cdot 7^2.$$

b) $a = 2\cdot 3\cdot 5\cdot 7$, $b = 7\cdot 11\cdot 13$. Thus
$$(a,b) = 7, \qquad \mathrm{LCM}(a,b) = 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13.$$

c) $a = 2^8\cdot 3^6\cdot 5^4\cdot 11^{13}$, $b = 2\cdot 3\cdot 5\cdot 11\cdot 13$. Thus
$$(a,b) = 2\cdot 3\cdot 5\cdot 11, \qquad \mathrm{LCM}(a,b) = 2^8\cdot 3^6\cdot 5^4\cdot 11^{13}\cdot 13.$$

d) $a = 41^{101}\cdot 47^{43}\cdot 103^{1001}$, $b = 41^{11}\cdot 43^{47}\cdot 83^{111}$. Thus
$$(a,b) = 41^{11}, \qquad \mathrm{LCM}(a,b) = 41^{101}\cdot 43^{47}\cdot 47^{43}\cdot 83^{111}\cdot 103^{1001}.$$

Exercise 34. Let $a,b\in\mathbb{Z}_{>0}$. Suppose that
$$(a,b) = 18 = 2\cdot 3^2 \quad \text{and} \quad \mathrm{LCM}(a,b) = 540 = 2^2\cdot 3^3\cdot 5.$$
Since $(a,b)\cdot\mathrm{LCM}(a,b) = ab$ we conclude that the possible prime factors of a, b are 2, 3 and 5. Write
$$a = 2^{d_2}3^{d_3}5^{d_5}, \quad b = 2^{e_2}3^{e_3}5^{e_5}, \quad d_i, e_i \geq 0$$
for the prime factorizations of a and b. We also know that
$$(a,b) = 2^{\min(d_2,e_2)}\cdot 3^{\min(d_3,e_3)}\cdot 5^{\min(d_5,e_5)}$$
and
$$\mathrm{LCM}(a,b) = 2^{\max(d_2,e_2)}\cdot 3^{\max(d_3,e_3)}\cdot 5^{\max(d_5,e_5)}.$$
Therefore,
$$\min(d_2,e_2) = 1 \qquad \max(d_2,e_2) = 2.$$
After interchanging a,b if necessary we can suppose $d_2 = 1$ and $e_2 = 2$. Similarly, we also have
$$\min(d_3,e_3) = 2,\ \max(d_3,e_3) = 3,\ \min(d_5,e_5) = 0,\ \max(d_5,e_5) = 1.$$
Thus $(d_3,e_3) = (2,3)$ or $(3,2)$ and $(d_5,e_5) = (1,0)$ or $(1,0)$, giving the following four possibilities for a,b:

(1) $a = 2^1\cdot 3^2 = 18$ and $b = 2^2\cdot 3^3\cdot 5^1 = 540$,
(2) $a = 2^1\cdot 3^2\cdot 5^1 = 90$ and $b = 2^2\cdot 3^3 = 108$,
(3) $a = 2^1\cdot 3^3 = 54$ and $b = 2^2\cdot 3^2\cdot 5^1 = 180$,
(4) $a = 2^1\cdot 3^3\cdot 5^1 = 270$ and $b = 2^2\cdot 3^2 = 36$,

Since (a,b) and $\mathrm{LCM}(a,b)$ do not depend on the signs and order of a,b we obtain all the solutions by multiplying a or b or both by -1 and interchanging them: $(\pm18,\pm540)$,$(\pm540,\pm18)$, $(\pm90,\pm108)$, $(\pm108,\pm90)$, $(\pm54,\pm180)$, $(\pm180,\pm54)$, $(\pm270,\pm36)$,$(\pm36,\pm270)$.

The following argument, avoiding the formula $(a,b)\cdot\mathrm{LCM}(a,b) = ab$, is an alternative to the first part of the proof above. Write
$$a = p_1^{e_1}\dots p_k^{e_k}, \qquad b = p_1^{d_1}\dots p_k^{d_k}, \qquad e_i, d_i \geq 0$$

(note that we have to allow the exponents to be zero so that we can use the same primes p_i in both factorizations). We have that

$$18 = 2 \cdot 3^2 = (a, b) = p_1^{\min(e_1,d_1)} \dots p_k^{\min(e_k,d_k)},$$

hence $p_1 = 2$, $\min(e_1, d_1) = 1$, $p_2 = 3$, $\min(e_2, d_2) = 2$ and $\min(e_i, d_i) = 0$ for all i satisfying $3 \le i \le k$. We also have,

$$540 = 2^2 3^3 5 = \mathrm{LCM}(a, b) = p_1^{\max(e_1,d_1)} \dots p_k^{\max(e_k,d_k)},$$

hence $\max(e_1, d_1) = 2$, $\max(e_2, d_2) = 3$, $p_3 = 5$, $\max(e_3, d_3) = 1$ and $\max(e_i, d_i) = 0$ for all i satisfying $4 \le i \le k$. Thus $e_i = d_i = 0$ for all i satisfying $4 \le i \le k$. Note this argument gives at the same time that the prime factors of a and b are 2, 3 or 5 and information about the possible exponents they may occur.

Exercise 42.

(a) Suppose $\sqrt[3]{5}$ is rational. Then, $\sqrt[3]{5} = a/b$ for some coprime positive integers a, b with $b \neq 0$. Then, we have

$$\sqrt[3]{5} = a/b \implies 5b^3 = a^3 \implies 5 \mid a$$

because 5 is a prime dividing the product $a^3 = aaa$, so divides one of the factors. Therefore, $a = 5k$ for some $k \in \mathbb{Z}$ and, replacing above gives

$$5b^3 = (5k)^3 \iff b^3 = 5^2k^3 \implies 5 \mid b,$$

showing that both a, b are divisible by 5, a contradiction.

(b) Let $f(x) = x^3 - 5$, which is a monic polynomial with integer coefficients. We have $f(\sqrt[3]{5}) = 0$ and since $\sqrt[3]{5}$ is not an integer it must be irrational by Theorem 3.18 (in the textbook).

Exercise 45. Suppose that $\log_p b$ is rational. Then, $\log_p b = r/q$ for some coprime $r, q \in \mathbb{Z}$ with $q \neq 0$. Then,

$$q \log_p b = r \implies (p^{\log_p b})^q = p^r \iff b^q = p^r$$

and since b is not a power of p it must be divisble by some other prime q. Then $q \mid p^r$, a contradiction since p is prime.

Exercise 56. We will work by contradiction.

Suppose there are only finitely many primes of the form $6k+5$. Denote them $p_0 = 5, p_1, \dots, p_k$ and consider the number

$$N = 6p_0p_1 \cdots p_k - 1.$$

Cleary $N > 1$ because $p_0 = 5$, so there exists a prime factor p dividing N. We apply the division algorithm to divide p by 6 and obtain

$$p = 6q + r, \qquad r, q \in \mathbb{Z}, \qquad 0 \le r \le 5.$$

We now divide into cases

(1) Suppose $r = 0, 2, 4$; then p is even, i.e $p = 2$. Since $2 \nmid N$ (it divides $N + 1$) this is impossible; thus $r \neq 0, 2, 4$.
(2) Suppose $r = 3$; then $3 \mid p$, i.e $p = 3$. Again, $3 \nmid N$, a contradiction.
(3) Suppose $r = 5$; thus p is of the form $6k+5$ and by hypothesis we have $p = p_i$ for some i. Since $p_i \mid N + 1$ it does not divide N, again a contradiction.

From these cases it follows that p is of the form $6k+1$. Since p is any prime factor of N, we conclude that all the prime factors occrring in the prime factorization of N are of the form $6k+1$. In other words,

$$N = \ell_1^{a_1} \cdot \ldots \cdot \ell_s^{a_s} \quad \text{with } \ \ell_i = 6k_i + 1 \ \text{ distinct primes and } \ a_i \geq 1.$$

Note that $(6k+1)(6k'+1) = 6(6kk'+k+k')+1$, that is the product of any two integers of the form $6k+1$ is also of this form. From the prime factorization above we conclude that N is of the form $6k+1$. This is incompatible with N being also of the form $6k-1$ as defined above. Thus our initial assumption is wrong, i.e. there are infinitely many primes of the form $6k+5$, as desired.

If you are familiar with congruences the last part of the proof can be restaded as follows. From the cases it follows that any prime q dividing N is of the form $6a+1$, that is $q \equiv 1 \pmod 6$. Since the product of two such primes q_1, q_2 (not necessatily distinct) also satisfies $q_1q_2 \equiv 1 \pmod 6$ we conclude that $N \equiv 1 \pmod 6$ which is a contradiction with $N \equiv -1 \equiv 5 \pmod 6$.

Section 3.7

Exercise 2. We apply the theorem we learned in class to describe solutions of linear Diophantine equations.

a) The equation $3x + 4y = 7$**.** Since $(3,4) = 1 \mid 7$ there are infinitely many solutions; note that $x_0 = y_0 = 1$ is a particular solution. Then all the solutions are of the form

$$x = 1 + 4t, \qquad y = 1 - 3t, \quad t \in \mathbb{Z}.$$

b) The equation $12x + 18y = 50$**.** Since $(12,18) = 6 \nmid 50$ there are no solutions.

c) The equation $30x + 47y = -11$**.** Clearly $(30,47) = 1$ (47 is prime) so there are solutions. We find a particular solution by applying the Euclidean algorithm followed by back substitution. Indeed,

$$47 = 30 \cdot 1 + 17, \qquad 30 = 17 \cdot 1 + 13, \qquad 17 = 13 \cdot 1 + 4$$

and

$$13 = 4 \cdot 3 + 1, \qquad 4 = 1 \cdot 4 + 0;$$

in particular, this double-checks that $(30,47) = 1$; we continue

$$\begin{aligned} 1 &= 13 - 4 \cdot 3 = 13 - (17-13) \cdot 3 = 13 \cdot 4 - 17 \cdot 3 = (30-17) \cdot 4 - 17 \cdot 3 = \\ &= 30 \cdot 4 - 17 \cdot 7 = 30 \cdot 4 - (47-30) \cdot 7 = 30 \cdot 11 - 47 \cdot 7. \end{aligned}$$

Thus $x_1 = 11$, $y_1 = -7$ is a particular solution to $30x + 47y = 1$. Thus $x_0 = -11x_1 = -121$, $y_0 = -11y_1 = 77$ is a particular solution to the desired equation. Therefore, the general solution is given by

$$x = -121 + 47t, \qquad y = 77 - 30t, \quad t \in \mathbb{Z}.$$

d) The equation $25x+95y = 970$**.** Since $(25,95) = 5 \mid 970$ there are infinitely many solutions. We divide both sides of the equation by 5 to obtain the equivalent equation

$$5x + 19y = 194.$$

Note that $(5,19) = 1$ and $x_1 = 4$, $y_1 = -1$ is a particular solution to $5x + 19y = 1$; then $x_0 = 194x_1 = 776$, $y_0 = 194y_1 = -194$ is a particular solution to our equation. Thus the general solution is given by

$$x = 776 + 19t, \qquad y = -194 - 5t, \quad t \in \mathbb{Z}.$$

e) The equation $102x+1001y = 1$**.** We find $(102, 1001)$ by applying the Euclidean algorithm:

$$1001 = 102 \cdot 9 + 83, \qquad 102 = 83 \cdot 1 + 19, \qquad 83 = 19 \cdot 4 + 7$$

and

$$19 = 7 \cdot 2 + 5, \qquad 7 = 5 \cdot 1 + 2, \qquad 5 = 2 \cdot 2 + 1,$$

hence $(102, 1001) = 1$ and the equation has infinitely many solutions. We apply back substitution to find a particular solution:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - (7-5) \cdot 2 = 7 \cdot (-2) + 5 \cdot 3 = 7 \cdot (-2) + (19 - 7 \cdot 2) \cdot 3 \\ &= 19 \cdot 3 - 7 \cdot 8 = 19 \cdot 3 - (83 - 19 \cdot 4) \cdot 8 = 83 \cdot (-8) + 19 \cdot 35 \\ &= 83 \cdot (-8) + (102 - 83) \cdot 35 = 102 \cdot 35 - 83 \cdot 43 = 102 \cdot 35 - (1001 - 102 \cdot 9) \cdot 43 \\ &= 1001 \cdot (-43) + 102 \cdot 422. \end{aligned}$$

Thus $x_0 = 422$, $y_0 = -43$ is a particular solution. Therefore, the general solution is given by

$$x = 422 + 1001t, \qquad y = -43 - 102t, \quad t \in \mathbb{Z}.$$

Exercise 6. This problem can be stated as finding a non-negative solution to the Diophantine equation $63x + 7 = 23y$, where x is the number of plantains in a pile, and y is the number of plantains each traveler receives.

Replace y by $-y$ and rearrange the equation into $63x + 23y = -7$ and note that $(63, 23) = 1$, hence there are infinitely many solutions. We apply Euclidean algorithm

$$63 = 23 \cdot 2 + 17, \quad 23 = 17 \cdot 1 + 6, \quad 17 = 6 \cdot 2 + 5, \quad 6 = 5 \cdot 1 + 1$$

and back substitution

$$\begin{aligned} 1 &= 6 - 5 = 6 - (17 - 6 \cdot 2) = 6 \cdot 3 - 17 = (23 - 17) \cdot 3 - 17 = \\ &= 23 \cdot 3 - 17 \cdot 4 = 23 \cdot 3 - (63 - 23 \cdot 2) \cdot 4 = 63 \cdot (-4) + 23 \cdot 11, \end{aligned}$$

hence $x_1 = -4$, $y_0 = 11$ is a particular solution to $63x + 23y = 1$. We conclude that $x_0 = -7x_1 = 28$, $y_0 = -7y_1 = -77$ is a particular solution. Thus the general solution is given by

$$x = 28 + 23t, \qquad y = -77 - 63t, \quad t \in \mathbb{Z}.$$

Replacing again y by $-y$ we get the general solution to $63x + 7 = 23y$ given by

$$x = 28 + 23t, \qquad y = 77 + 63t, \quad t \in \mathbb{Z}.$$

These values of x, y are both positive when $t \geq -1$, therefore the number of plantains in the pile could be any integer of the form $28 + 23t$ for $t \geq -1$.

SOLUTIONS TO PROBLEM SET 2

Section 4.1

Exercise 4. Let $a \in \mathbb{Z}$.

Suppose a is even; then $a \equiv 0 \pmod 4$ or $a \equiv 2 \pmod 4$. Since $0^2 = 0 \equiv 0 \pmod 4$ and $2^2 = 4 \equiv 0 \pmod 4$ we conclude $a^2 \equiv 0 \pmod 4$.

Suppose a is odd; then $a \equiv 1 \pmod 4$ or $a \equiv 3 \pmod 4$. Since $1^2 = 1 \equiv 1 \pmod 4$ and $3^2 = 9 \equiv 1 \pmod 4$ we conclude $a^2 \equiv 1 \pmod 4$.

Exercise 30. We will use induction to show that $4^n \equiv 1 + 3n \pmod 9$ for all $n \in \mathbb{Z}_{\geq 0}$.

Base $n = 0$: $4^0 = 1 \equiv 1 = 1 + 3 \cdot 0 \pmod 9$.

Hypothesis: The result holds for n.

Step $n+1$: We have

$$\begin{aligned} 4^{n+1} &= 4 \cdot 4^n \equiv 4(1+3n) \equiv 4 + 12n \pmod 9 \\ &\equiv 4 + 3n \equiv 1 + 3(n+1) \pmod 9, \end{aligned}$$

as desired; we used the induction hypothesis in the first congruence.

Exercise 36. Note that the smallest power of 2 which is larger than all the exponents in this exercise is $2^8 = 256$. Therefore, we will repeatedly square and reduce modulo 47 to compute $2^i \pmod{47}$ for $1 \leq i \leq 7$. Indeed, we have

$$\begin{aligned} 2^1 &= 2 \equiv 2 \pmod{47} \\ 2^2 &= 4 \equiv 4 \pmod{47} \\ 2^4 &= 16 \equiv 16 \pmod{47} \\ 2^8 &= 256 \equiv 21 \pmod{47} \\ 2^{16} &\equiv 21^2 \equiv 18 \pmod{47} \\ 2^{32} &\equiv 18^2 \equiv 42 \pmod{47} \\ 2^{64} &\equiv 42^2 \equiv 25 \pmod{47} \\ 2^{128} &\equiv 25^2 \equiv 14 \pmod{47}. \end{aligned}$$

a) Compute 2^{32}: We have seen above that $2^{32} \equiv 42 \pmod{47}$

b) Compute 2^{47}: Since $47 = 32 + 8 + 4 + 2 + 1$, we have

$$2^{47} = 2^{32}2^8 2^4 2^2 2^1 \equiv 42 \cdot 21 \cdot 16 \cdot 4 \cdot 2 \equiv 2 \pmod{47}.$$

c) Compute 2^{200}: Since $200 = 128 + 64 + 8$, we have

$$2^{200} = 2^{128}2^{64}2^8 \equiv 14 \cdot 25 \cdot 21 \equiv 18 \pmod{47}.$$

Exercise 2. We will apply the theorem from class that fully describes the solutions of linear congruences.

a) Solve $3x \equiv 2 \pmod 7$**.** Since $(3,7) = 1$ there is exactly one solution mod 7. Since $3{\cdot}3 = 9 \equiv 2 \pmod 7$ we conclude that $x \equiv 3 \pmod 7$ is the unique solution of the congruences.

b) Solve $6x \equiv 3 \pmod 9$**.** Since $(6,9) = 3$ there are exactly three non-congruent solutions mod 9. Note that $x_0 \equiv 2 \pmod 9$ is a particular solution; then $x \equiv 2 - (9/3)t = 2 - 3t$ with $0 \le t \le 2$ give all the non-congruent solutions. Indeed, $t = 0,1,2$ respectively correspond to the solutions $x \equiv 2,8,5 \pmod 9$.

c) Solve $17x \equiv 14 \pmod{21}$**.** Since $(17,21) = 1$ there is exactly one solution. We know that the solution will correspond to the x-coordinate of a particular solution of the Diophantine equation $17x - 21y = 14$. We compute it by applying the Euclidean algorithm and back substitution:

$$21 = 17 \cdot 1 + 4, \quad 17 = 4 \cdot 4 + 1, \quad 4 = 4 \cdot 1 + 0$$

and

$$1 = 17 - 4 \cdot 4 = 17 - (21 - 17) \cdot 4 = 17 \cdot 5 - 21 \cdot 4,$$

hence $x_1 = 5$, $y_1 = 4$ is a solution to $17x - 21y = 1$. Therefore, $x_0 = 14x_1 = 14 \cdot 5 = 70$, $y_0 = 14y_1 = 14 \cdot 4 = 56$ is a particular solution to $17x - 21y = 14$. It follows that $x \equiv x_0 \equiv 7 \pmod{21}$ is the unique solution to the congruence.

d) Solve $15x \equiv 9 \pmod{25}$**.** Since $(15,25) = 5$ and $5 \nmid 9$ there are no solutions to the congruence.

Exercise 6. The congruence $12x \equiv c \pmod{30}$ has solutions if and only if $(12,30) = 6$ divides c. In the range $0 \le c < 30$ this occurs for $c = 0,6,12,18,24$ in which cases there are 6 non-congruent solutions.

Exercise 8. Since 13 is a small number we can solve this exercise by trial and error.

a) Since $7 \cdot 2 = 14 \equiv 1 \pmod{13}$ we have $2^{-1} \equiv 7 \pmod{13}$.

b) Since $9 \cdot 3 = 27 \equiv 1 \pmod{13}$ we have $3^{-1} \equiv 9 \pmod{13}$.

c) Since $8 \cdot 5 = 40 \equiv 1 \pmod{13}$ we have $5^{-1} \equiv 8 \pmod{13}$.

d) Since $6 \cdot 11 = 66 \equiv 1 \pmod{13}$ we have $11^{-1} \equiv 6 \pmod{13}$.

Exercise 10.

a) An integer a will have an inverse mod 14 if and only if $ax \equiv 1 \pmod{14}$ has a solution, that is exactly when $(a,14) = 1$. The numbers a in the interval $1 \le a \le 14$ satisfying this condition are $\{1,3,5,9,11,13\}$.

b) Note that the inverse of a^{-1} is a so the inverse of $a \in \{1,3,5,9,11,13\}$ must also belong to this list since it contains all the invertible elements mod 14. Finally, note that

$$1 \cdot 1 \equiv 1, \quad 3 \cdot 5 = 15 \equiv 1, \quad 9 \cdot 11 = 99 \equiv 1, \quad 13 \cdot 13 = 169 \equiv 1 \pmod{14}$$

which means that

$$1^{-1} \equiv 1, \qquad 3^{-1} \equiv 5, \qquad 5^{-1} \equiv 3 \pmod{14}$$

and

$$9^{-1} \equiv 11, \qquad 11^{-1} \equiv 9, \qquad 13^{-1} \equiv 13 \pmod{14}.$$

Section 4.3

Exercise 2. The question is equivalent to find a solution to the congruences

$$x \equiv 1 \pmod 2, \quad x \equiv 1 \pmod 5, \quad x \equiv 0 \pmod 3.$$

The unique modulo 10 solution of the first two congruences is $x \equiv 1 \pmod{10}$. Thus the original system is equivalent to

$$x \equiv 1 \pmod{10}, \quad x \equiv 0 \pmod 3.$$

We rewrite the first congruence as an equality, namely $x = 1 + 10t$, where t is an integer. Inserting this expression for x into the second congruence, we find that

$$1 + 10t \equiv 0 \pmod 3 \quad \Leftrightarrow \quad t \equiv 2 \pmod 3,$$

which means $t = 2 + 3s$, where s is an integer. Hence any integer $x = 1 + 10t = 1 + 10(2 + 3s) = 21 + 30s$ will be a solution to the problem. For example, taking $s = 0$ we get $x = 21$. In the language of congruences, we have shown that

$$x \equiv 21 \pmod{30},$$

is the unique solution mod 30.

We now solve this exercise by applying the CRT to the congruences

$$x \equiv 1 \pmod{10}, \quad x \equiv 0 \pmod 3.$$

Indeed, we have $b_1 = 1$, $b_2 = 0$, $n_1 = 10$, $n_2 = 3$, $M = n_1 n_2 = 30$, $M_1 = M/n_1 = 3$ and $M_2 = M/n_2 = 10$; the formula for the unique solution modulo M gives

$$x = b_1 M_1 y_1 + b_2 M_2 y_2 = 1 \cdot M_1 \cdot y_1 + 0 \cdot M_2 \cdot y_2 = 3y_1,$$

where y_1 is satisfies $M_1 y_1 \equiv 1 \pmod{n_1}$, that is $y_1 = 3^{-1} \pmod{10} = 7 \pmod{10}$. We conclude that

$$x = 3 \cdot 7 = 21 \pmod{30},$$

as expected.

Exercise 4. We will use the CRT.

a) Solve

$$x \equiv 4 \pmod{11}, \qquad x \equiv 3 \pmod{17}.$$

We have $(11, 17) = 1$. We have $b_1 = 4$, $b_2 = 3$, $n_1 = 11$, $n_2 = 17$, $M = n_1 n_2 = 187$, $M_1 = M/n_1 = 17$ and $M_2 = M/n_2 = 11$; furthermore, we determine y_1, y_2 by solving the congruences $M_i y_i \equiv 1 \pmod{n_i}$, that is

$$17y_1 \equiv 1 \pmod{11} \quad \text{and} \quad 11y_2 \equiv 1 \pmod{17}.$$

Both y_i can be found by solving the Diophantine equation $17y_1 + 11y_2 = 1$. We only need a particular solution, and one is easy to find by trial and error: $y_1 = 2, y_2 = -3$. Now

$$x = b_1 \cdot M_1 \cdot y_1 + b_2 \cdot M_2 \cdot y_2 = 4 \cdot 17 \cdot 2 + 3 \cdot 11 \cdot (-3) = 37.$$

Thus $x = 37$ is the unique solution modulo $M = 187$.

b) Note that 2, 3 and 5 are pairwise coprime. The first two equations can be rewritten as

$$x \equiv -1 \pmod 2, \qquad x \equiv -1 \pmod 3$$

and by the CRT they are equivalent to $x \equiv -1 \pmod 6$. Thus our system of congruences is equivalent to

$$x \equiv -1 \pmod 6, \qquad x \equiv 3 \pmod 5.$$

We have $b_1 = -1$, $b_2 = 3$, $n_1 = 6$, $n_2 = 5$, $M = n_1 n_2 = 30$, $M_1 = M/n_1 = 5$ and $M_2 = M/n_2 = 6$; furthermore, we easily find that

$$y_1 = 5^{-1} \equiv -1 \pmod 6 \quad \text{and} \quad y_2 = 6^{-1} \equiv 1 \pmod 5.$$

Thus by the formula for the unique solution is

$$x \equiv (-1) \cdot 5 \cdot (-1) + 3 \cdot 6 \cdot 1 \equiv 23 \pmod{30}.$$

c) By looking at the congruences it is easy to see that $x = 6$ satisfies all of them. Thus by the CRT we have an unique solution $x \equiv 6 \pmod{210}$, since $210 = 2 \cdot 3 \cdot 5 \cdot 7$ and 2, 3, 5 and 7 are pairwise coprime.

Alternatively, we can apply the formula

$$x \equiv 0 \cdot M_1 \cdot y_1 + 0 \cdot M_2 \cdot y_2 + 1 \cdot M_3 \cdot y_3 + 6 \cdot M_4 \cdot y_4 \pmod{210},$$

where $M_3 = 210/5 = 42$ and $M_4 = 210/7 = 30$. To determine y_3, we solve $42 y_3 \equiv 1 \pmod 5$, or equivalently $y_3 = 42^{-1} \equiv 2^{-1} \equiv 3 \mod 5$. To determine y_4, we solve $30 y_4 \equiv 1 \pmod 7$, or equivalently $y_4 = 30^{-1} \equiv 2^{-1} \equiv 4 \mod 7$. Now $x \equiv 1 \cdot 42 \cdot 3 + 6 \cdot 30 \cdot 4 \equiv 6 \pmod{210}$, as expected.

Exercise 22. If x is the number of gold coins, the problem is equivalent to finding the least positive solution to the following system of congruences:

$$\begin{aligned} x &\equiv 3 \pmod{17} \\ x &\equiv 10 \pmod{16} \\ x &\equiv 0 \pmod{15}. \end{aligned}$$

As $17, 16$, and 15 are pairwise coprime, we can use the CRT to find the unique solution modulo $M = 15 \cdot 16 \cdot 17 = 4080$. Thus the solution is given by the formula

$$x = 3 \cdot M_1 \cdot y_1 + 10 \cdot M_2 \cdot y_2 + 0 \cdot M_3 \cdot y_3 \equiv 3 \cdot M_1 \cdot y_1 + 10 \cdot M_2 \cdot y_2 \pmod M,$$

where $M_1 = 15 \cdot 16 = 240$, $M_2 = 15 \cdot 17 = 255$, y_1 is a solution to the congruence

$$(15 \cdot 16) y \equiv 1 \pmod{17} \iff (-2) \cdot (-1) y \equiv 2y \equiv 1 \pmod{17}$$

and y_2 is a solution to

$$(15 \cdot 17) y \equiv 1 \pmod{16} \iff (-1) \cdot 1 y \equiv -y \equiv 1 \pmod{16}.$$

Thus, we can take $y_1 = 9$ and $y_2 = -1$, obtaining

$$x = 3 \cdot 240 \cdot 9 + 10 \cdot 255 \cdot (-1) = 3930 \pmod{4080}.$$

We conclude that, the number of coins can be $3930 + 4080n$ where n is a non-negative integer; the smallest such number is 3930.

Exercise 2.

a) The last 3 digits of 112250 are 250 which is divisible by $5^3 = 125$, but the last 4 digits are 2250 which is not divisible by $5^4 = 625$. Thus the largest power of 5 dividing 112250 is 3.

b) The last 4 digits of 4860625 are 0625 which is divisible by $5^4 = 625$, but the last 5 digits are 60625, which is not divisible by $5^5 = 3125$. Thus the largest power of 5 dividing 4860625 is 4.

c) The last 2 digits of 235555790 are 90 which is not divisible by $5^2 = 25$, but 235555790 is divisible by 5, so the largest power of 5 dividing 235555790 is 1.

d) The last 5 digits of 48126953125 are 53125 which is divisible by $5^5 = 3125$. Dividing 48126953125 by $5^5 = 3125$, we get 15400625. This number is divisible by $5^4 = 625$ but not $5^5 = 3125$. Thus the highest power of 5 dividing 48126953125 is $5 + 4 = 9$.

Exercise 4. A number is divisible by 11 if and only if the integer formed by alternatively sum of its digits is divisible by 11. We use this to test divisibility.

a)

$$1 - 0 + 7 - 6 + 3 - 7 + 3 - 2 = -1$$

so 10763732 is not divisible by 11.

b)

$$1 - 0 + 8 - 6 + 3 - 2 + 0 - 0 + 1 - 5 = 0$$

so 1086320015 is divisible by 11.

c)

$$6 - 7 + 4 - 3 + 1 - 0 + 9 - 7 + 6 - 3 + 7 - 5 = 8$$

so 674310976375 is not divisible by 11.

d)

$$8 - 9 + 2 - 4 + 3 - 1 + 0 - 0 + 6 - 4 + 5 - 3 + 7 = 10$$

so 8924310064537 is not divisibly by 11.

Exercise 22. We know that the total cost being $x42y$ cents is divisible by $88 = 8 \cdot 11$ and so is divisible by both 11 and $2^3 = 8$. Thus $42y$ is divisible by $2^3 = 8$, and so $2y$ is divisible by $2^2 = 4$ and y is divisible by 2. The only number $0 \leq y < 10$ satisfying this is $y = 4$. As $x424$ is divisible by 11 we require that

$$x - 4 + 2 - 4 = x - 6$$

is divisible by 11. The only number $0 \leq x < 10$ satisfying this is $x = 6$. Thus the total cost was \$64.24 and each chicken cost \$64.24/88 = \$0.73.

Exercise 12. We use the fact that

$$\sum_{i=1}^{10} i x_i \equiv 0 \mod 11.$$

a) We have

$$1\cdot 0 + 2\cdot 1 + 3\cdot 9 + 4\cdot 8 + 5\cdot x_5 + 6\cdot 3 + 7\cdot 8 + 8\cdot 0 + 9\cdot 4 + 10\cdot 9 \equiv 5x_2 + 8 \equiv 0 \pmod{11}.$$

Thus $x_5 \equiv (-8)\cdot 5^{-1} \equiv 3\cdot 9 \equiv 5 \pmod{11}$, and the missing digit is $x_5 = 5$.

b) We have

$$1\cdot 9 + 2\cdot 1 + 3\cdot 5 + 4\cdot 5 + 5\cdot 4 + 6\cdot 2 + 7\cdot 1 + 8\cdot 2 + 9\cdot x_9 + 10\cdot 6 \equiv 9x_9 + 7 \equiv 0 \pmod{11}.$$

Thus $x_9 \equiv (-7)\cdot 9^{-1} \equiv 4\cdot 5 \equiv 9 \pmod{11}$, and the missing digit is $x_9 = 9$.

c) We have

$$1\cdot x_1 + 2\cdot 2 + 3\cdot 6 + 4\cdot 1 + 5\cdot 0 + 6\cdot 5 + 7\cdot 0 + 8\cdot 7 + 9\cdot 3 + 10\cdot 10 \equiv x_1 + 8 \equiv 0 \pmod{11}.$$

Thus $x_1 \equiv -8 \equiv 3 \pmod{11}$, and the missing digit is $x_1 = 3$.

Exercise 13. Let x_i denote the digits of $0-07-289095-0$ which is an ISBN10 code obtained by transposing two digits of a valid ISBN10 code. Let S denote the sum

$$S = \sum_{i=1}^{10} i x_i = 3\cdot 7 + 4\cdot 2 + 5\cdot 8 + 6\cdot 9 + 7\cdot 0 + 8\cdot 9 + 9\cdot 5 + 10\cdot 0 \equiv 9 \pmod{11},$$

hence $S \not\equiv 0 \pmod{11}$ (as expected, since the code is invalid).

Let S' denote the sum corresponding to the original code. We have $S' \equiv 0 \pmod{11}$. Suppose that the j^{th} and k^{th} digits were transposed. Then, to reconstruct S' from S, we subtract the incorrectly positioned digits and add the correct ones, that is

$$S' = S - jx_j - kx_k + jx_k + kx_j = S + (j-k)(x_k - x_j).$$

Now, $S' \equiv S + (j-k)(x_k - x_j) \pmod{11}$ is equivalent to

$$0 \equiv 9 + (j-k)(x_k - x_j) \pmod{11} \iff (j-k)(x_k - x_j) \equiv -9 \pmod{11}.$$

By trial and error we find that this is satisfied by $j = 7, k = 8$ and no other cases. Thus the correct ISBN-10 is $0 - 07 - 289905 - 0$.

SOLUTIONS TO PROBLEM SET 3

Section 6.1

Exercise 4. We want to find $r \in \mathbb{Z}$ such that

$$5!25! \equiv r \pmod{31} \quad \text{and} \quad 0 \le r \le 30.$$

By Wilson's theorem $30! \equiv -1 \pmod{31}$. Then,

$$5!25! \equiv 25! \cdot (-26) \cdot (-27) \cdot (-28) \cdot (-29) \cdot (-30) \equiv (-1)^5 30! \equiv (-1)^6 \equiv 1 \pmod{31},$$

that is $r = 1$.

Exercise 10. We want to find $r \in \mathbb{Z}$ such that

$$6^{2000} \equiv r \pmod{11} \quad \text{and} \quad 0 \le r \le 10.$$

Since 11 is prime and $(6,11) = 1$ by Fermat's little theorem we have $6^{10} \equiv 1 \pmod{11}$. Then,

$$6^{2000} = (6^{10})^{200} \equiv 1^{200} \equiv 1 \pmod{11},$$

thus $r = 1$.

Exercise 12. We want to find $r \in \mathbb{Z}$ such that

$$2^{1000000} \equiv r \pmod{17} \quad \text{and} \quad 0 \le r \le 16.$$

Since 17 is prime and $(2,17) = 1$ by FLT we have $2^{16} \equiv 1 \pmod{17}$. Then,

$$2^{1000000} = (2^{16})^{2^2 \cdot 5^6} \equiv 1 \pmod{17},$$

thus $r = 1$.

Exercise 24. It is a corollary of FLT that $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$. Then

$$1^p + 2^p + 3^p + \ldots + (p-1)^p \equiv 1 + 2 + 3 + \ldots + (p-1) \pmod{p}.$$

Note that since p is odd $p-1$ is even and

$$p - \frac{p-1}{2} = \frac{2p-p+1}{2} = \frac{p+1}{2}.$$

Moreover, we can rearrange the sum above as the following sum of $(p-1)/2$ terms

$$\begin{aligned} 1 + 2 + 3 + \ldots + (p-1) &\equiv (1 + (p-1)) + (2 + (p-2)) + \ldots + (\frac{p-1}{2} + \frac{p+1}{2}) \pmod{p} \\ &\equiv p + p + \ldots p \equiv 0 \pmod{p}. \end{aligned}$$

Section 6.2

Exercise 2. Note that $45 = 9 \cdot 5$ is composite and $(17, 45) = (19, 45) = 1$.

We have

$$17^4 \equiv 2^4 \equiv 16 \equiv 1 \pmod 5 \qquad \text{and} \qquad 17^4 \equiv (-1)^4 \equiv 1 \pmod 9.$$

Since $(5, 9) = 1$ the CRT implies that $17^4 \equiv 1 \pmod{45}$, therefore

$$17^{44} = (17^4)^{11} \equiv 1 \pmod{45}$$

and we conclude 45 is a pseudoprime for the base 17.

We have

$$19^2 \equiv (-1)^2 \equiv 1 \pmod 5 \qquad \text{and} \qquad 19^2 \equiv 1^2 \equiv 1 \pmod 9.$$

Since $(5, 9) = 1$ the CRT implies that $19^2 \equiv 1 \pmod{45}$, therefore

$$19^{44} = (19^2)^{22} \equiv 1 \pmod{45}$$

and we conclude 45 is a pseudoprime for the base 19.

Exercise 8. Let p be prime and write $N = 2^p - 1$.

Suppose N is composite; hence $p \geq 3$. Since $(2, p) = 1$ we have $2^{p-1} \equiv 1 \pmod p$ by FLT and so $2^{p-1} - 1 = pk$ for some odd $k \in \mathbb{Z}$. Thus

$$N - 1 = 2^p - 2 = 2(2^{p-1} - 1) = 2pk.$$

Note also that $2^p = N + 1 \equiv 1 \pmod N$; thus

$$2^{N-1} = 2^{2pk} = (2^p)^{2k} \equiv 1 \pmod N,$$

that is N is a pseudoprime to the base 2.

Exercise 12. An odd composite $N > 0$ is a strong pseudoprime for the base b if it fools Miller's Test in base b. Recall that to be possible to apply the $(k+1)$-th step of Miller's test in base b we need

$$b^{(N-1)/2^k} \equiv 1 \pmod N \qquad \text{and} \qquad N - 1 \text{ is divisible by } 2^{k+1}.$$

Let $N = 25$. We have $N - 1 = 25 - 1 = 24 = 2^3 \cdot 3$. We first observe that

$$7^6 = (7^2)^3 \equiv 49^3 \equiv (-1)^3 \equiv -1 \pmod{25}.$$

We now apply Miller's test

$$\begin{aligned} 7^{24} &\equiv (7^6)^4 \equiv (-1)^4 \equiv 1 \pmod{25} \quad \text{(i.e. 25 is a pseudoprime to base 7)}, \\ 7^{12} &\equiv (7^6)^2 \equiv (-1)^2 \equiv 1 \pmod{25}, \\ 7^6 &\equiv -1 \pmod{25}; \end{aligned}$$

despite the fact that 6 is divisible by 2 the last congruence means we have to stop.

Therefore 25 fools the test, i.e. it is a strong pseudoprime to the base 7.

Exercise 18.

a) Let $m \in \mathbb{Z}_{>0}$ be such that $6m+1$, $12m+1$ and $18m+1$ are prime numbers. Write $n = (6m+1)(12m+1)(18m+1)$ and let $b \in \mathbb{Z}_{\geq 2}$ satisfy $(b,n) = 1$.

As $6m+1 \mid n$ we also have $(6m+1, b) = 1$ hence $b^{6m} \equiv 1 \pmod{6m+1}$ by FLT. Similarly, we conclude also that

$$b^{12m} \equiv 1 \pmod{12m+1} \quad \text{and} \quad b^{18m} \equiv 1 \pmod{18m+1}.$$

Now note that

$$n = 6 \cdot 12 \cdot 18 m^3 + (6 \cdot 12 + 6 \cdot 18 + 12 \cdot 18)m^2 + 36m + 1$$

then $6m \mid n-1$, $12m \mid n-1$ and $18m \mid n-1$. Thus the following congruence hold

$$\begin{aligned} b^{n-1} &\equiv 1 \pmod{6m+1} \\ b^{n-1} &\equiv 1 \pmod{12m+1} \\ b^{n-1} &\equiv 1 \pmod{18m+1} \end{aligned}$$

and since $6m+1$, $12m+1$ and $18m+1$ are pairwise coprime (because they are distinct primes) by CRT we conclude that $b^{n-1} \equiv 1 \pmod{n}$. Since b was arbitrary we conclude that n is a Carmichael number.

Alternative proof using Korset's criterion: Let m be a positive integer such that $6m+1$, $12m+1$, and $18m+1$ are primes. Then the number $n = (6m+1)(12m+1)(18m+1)$ is squarefree. Let $p \mid n$ be a prime. Then $p - 1 = 6m, 12m$ or $18m$. Now note that

$$n = 6 \cdot 12 \cdot 18 m^3 + (6 \cdot 12 + 6 \cdot 18 + 12 \cdot 18)m^2 + 36m + 1$$

then $6m \mid n-1$, $12m \mid n-1$ and $18m \mid n-1$. We conclude that for all primes $p \mid n$ we have $p - 1 \mid n - 1$, hence n is a Carmichael number by Korset's criterion.

b) Take respectively $m = 1, 6, 35, 45, 51$.

Section 6.3

Exercise 6. The question is equivalent to find $r \in \mathbb{Z}$ such that

$$7^{999999} \equiv r \pmod{10} \quad \text{and} \quad 0 \leq r \leq 9.$$

Since $(7, 10) = 1$ and $\phi(10) = 4$ then $7^4 \equiv 1 \pmod{10}$ by Euler's theorem.

Note that $999996 = 4 \cdot 249999$, then

$$7^{999999} = 7^{999996} \cdot 7^3 = (7^4)^{249999} \cdot 7^3 \equiv 1 \cdot 7^3 \equiv 343 \equiv 3 \pmod{10},$$

hence $r = 3$ is the last digit of the decimal expansion.

Remark: For the argument above we do not need the factorization $999996 = 4 \cdot 249999$. It is enough to know that $4 \mid 999996$ which one can check (for example) using the criterion for divisibility by 4. Indeed, write $999996 = 4k$; then

$$7^{999999} = 7^{999996} \cdot 7^3 = (7^4)^k \cdot 7^3 \equiv 343 \equiv 3 \pmod{10},$$

as above. This is relevant because sometimes it allows to work with very large numbers without having to find factorizations.

Exercise 8. Let $a \in \mathbb{Z}$ satisfy $3 \nmid a$ or $9 \mid a$.

It is a consequence of FLT that $a^7 \equiv a \pmod 7$. We claim that $a^7 \equiv a \pmod 9$. Note that $63 = 7 \cdot 9$ and $(7, 9) = 1$. Then by the CRT we conclude that $a^7 \equiv a \pmod{63}$, as desired.

We will now prove the claim, dividing into two cases:

(i) Suppose $9 \mid a$; then $9 \mid a^7$ and $a^7 \equiv 0 \equiv a \pmod 9$.
(ii) Suppose $3 \nmid a$; then $(a, 9) = 1$. We have $\phi(9) = 6$ and by Euler's theorem we have $a^6 \equiv 1 \pmod 9$. Thus $a^7 \equiv a \pmod 9$, as desired.

Exercise 10. Let $a, b \in \mathbb{Z}_{>0}$ be coprime. We have

$$a^{\phi(b)} \equiv 1 \pmod b, \qquad a^{\phi(b)} \equiv 0 \pmod a$$

and

$$b^{\phi(a)} \equiv 1 \pmod a, \qquad b^{\phi(a)} \equiv 0 \pmod b.$$

Thus we also have

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod a, \qquad a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod b$$

and by the CRT we conclude $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$, as desired.

Exercise 14. We know from the proof of CRT that the unique solution modulo $M = m_1 \cdot \ldots \cdot m_n$ to the system of congruences is given by

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_r M_r y_r \pmod M$$

where $M_i = M/m_i$ and $y_i \in \mathbb{Z}$ satisfies $M_i y_i \equiv 1 \pmod{m_i}$. Now note that $(M_i, m_i) = 1$ and Euler's theorem implies

$$M_i^{\phi(m_i)} = M_i \cdot M_i^{\phi(m_i)-1} \equiv 1 \pmod{m_i},$$

hence we can take $y_i = M_i^{\phi(m_i)-1}$. Inserting in the formula for x we get

$$x = a_1 M_1^{\phi(m_1)} + a_2 M_2^{\phi(m_2)} + \ldots + a_r M_r^{\phi(m_r)} \pmod M,$$

as desired.

Section 7.1

Exercise 4. Let ϕ be the Euler ϕ-function. Let $n \in \mathbb{Z}_{>0}$. If $n \neq 1$ it has a prime factorization $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ where $a_k \geq 1$ and p_i are distinct primes. We have

$$\phi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1).$$

a) Suppose $\phi(n) = 1$. Since $\phi(1) = 1$ then $n = 1$ is a solution. Suppose $n \neq 1$. From the formula above it follows that $p_i - 1 = 1$ for all i; thus 2 is the unique prime factor of n, that is $n = 2^{a_1}$. Again by the formula we have $1 = \phi(2^{a_1}) = 2^{a_1 - 1}$ which implies $a_1 = 1$, hence $n = 2$.

Thus $\phi(n) = 1$ if and only if $n = 1$ or $n = 2$.

b) Suppose $\phi(n) = 2$; thus $n \neq 1$. By the formula $p_i - 1 \mid 2$ for all i; thus only the primes 2 and 3 can divide n. Write $n = 2^{a_1} 3^{a_2}$; if $a_2 \neq 0$ from the formula we have $3^{a_2 - 1} \mid 2$ thus $a_2 = 1$. We conclude that $a_2 = 0$ or $a_2 = 1$. We now divide into two cases:

(i) Suppose $a_2 = 1$, i.e. $n = 2^{a_1} \cdot 3$. If $a_1 \geq 2$ then the formula shows that $\phi(n) = 2$ is divisible by 4, a contradiction. We conclude $a_1 \leq 1$, that is $n = 3$ or $n = 6$. Both are solutions because $\phi(3) = \phi(6) = 2$.

(ii) Suppose $a_2 = 0$, i.e $n = 2^{a_1}$ with $a_1 \geq 1$. Then $\phi(n) = 2^{a_1-1} = 2$ implies $a_1 = 2$, that is $n = 4$.

Thus $\phi(n) = 2$ if and only if $n = 3$, $n = 4$ or $n = 6$.

c) Suppose $\phi(n) = 3$ (hence $n \neq 1$). Then $p_i - 1 = 1$ or 3 for all i. Since $p_i = 4$ is not a prime we conclude that $p_i - 1 = 1$; thus only the prime 2 divide n, that is $n = 2^{a_1}$ with $a_1 \geq 1$. Therefore $\phi(n) = 2^{a_1-1} = 3$ which is impossible for any value of a_1.

Thus there are no solutions to $\phi(n) = 3$.

d) Suppose $\phi(n) = 4$ (hence $n \neq 1$). Again, the formula shows that $p_i - 1 \mid 4$ for all i; thus only the primes 2, 3 and 5 can divide n, that is $n = 2^{a_1}3^{a_2}5^{a_3}$ with at least one exponent ≥ 1. If $a_2 \geq 2$ then $3 \mid \phi(n) = 4$, a contradiction; thus $a_2 \leq 1$. We now divide into the cases:

(i) Suppose $a_2 = 1$, i.e. $n = 2^{a_1} \cdot 3 \cdot 5^{a_3}$. Then

$$4 = \phi(n) = \phi(3)\phi(2^{a_1}5^{a_3}) = 2\phi(2^{a_1}5^{a_3})$$

and we conclude $\phi(2^{a_1}5^{a_3}) = 2$. By part (b) the only integers m such that $\phi(m) = 2$ are $m = 3, 4, 6$ and among these only $m = 4$ is of the form $2^{a_1}5^{a_3}$. We conclude that $a_1 = 2$ and $a_3 = 0$ therefore $n = 3 \cdot 4 = 12$.

(ii) Suppose $a_2 = 0$, i.e. $n = 2^{a_1}5^{a_3}$. Clearly, $a_3 \leq 1$ otherwise $5 \mid \phi(n) = 4$.

Suppose $a_3 = 1$, that is $n = 2^{a_1} \cdot 5$. If $a_1 = 0$ then $n = 5$ and $\phi(5) = 4$ is a solution; if $a_1 \geq 1$ then $4 = \phi(n) = 2^{a_1-1} \cdot 4$ implies $a_1 = 1$, that is $n = 10$.

Suppose $a_3 = 0$, that is $n = 2^{a_1}$ with $a_1 \geq 1$. Thus $\phi(n) = 2^{a_1-1} = 4$ implies $a_1 = 3$ that is $n = 8$.

Thus $\phi(n) = 4$ if and only if $n = 5, 8, 10$ or 12.

Exercise 8. Suppose $\phi(n) = 14$; hence $n > 1$. Consider the prime factorization $n = p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$ where $a_k \geq 1$ and p_i are distinct primes. We have

$$\phi(n) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1).$$

From the formula it follows $p_i - 1 \mid 14$ for each prime $p_i \mid n$, that is $p_i - 1 \in \{1, 2, 7, 14\}$; thus $p_i = 2, 3, 8, 15$ and we conclude that only the primes 2 and 3 can divide n. Write $n = 2^{a_1}3^{a_2}$. We have $\phi(n) = \phi(2^{a_1})\phi(3^{a_2}) = 14$, but from the formula we see that $7 \nmid \phi(2^{a_1})$ and $7 \nmid \phi(3^{a_2})$, a contradiction.

Thus $\phi(n) = 14$ has no solutions.

Exercise 18. Let $n \in \mathbb{Z}_{>0}$ be odd; then $(4, n) = 1$. Since ϕ is a multiplicative function we have $\phi(4n) = \phi(4)\phi(n) = 2\phi(n)$, as desired.

SOLUTIONS TO PROBLEM SET 4

Section 7.2

Exercise 4. Let $n \in \mathbb{Z}_{>0}$ and consider its prime decomposition $n = 2^d p_1^{d_1} \cdots p_r^{d_r}$, where p_i are distinct odd primes. As σ is multiplicative, we have

$$\sigma(n) = \sigma(2^d)\sigma(p_1^{d_1}) \cdots \sigma(p_r^{d_r}).$$

Thus $\sigma(n)$ is odd if and only if all its factors above, which are of the form $\sigma(p^k)$ where p is a prime, are odd. For any prime p we have $\sigma(p^k) = 1 + p + \cdots + p^k$ which is odd if and only if $p + \cdots + p^k$ is even. This is the case when $p = 2$ or if p is odd but we have an even number of odd terms in the sum, that is k even.

Thus $\sigma(n)$ is odd if and only if each odd prime p dividing n occurs with an even exponent in the prime factorization of n. That is, the sum of the divisors of n is odd if and only if n is of the form $n = 2^d p_1^{d_1} \cdots p_r^{d_r}$ with $d_i = 2d_i'$ for all i. Equivalently, when n is of the form $2^d m^2$ for some odd integer m.

Exercise 7. Let p be a prime number and $a \in \mathbb{Z}_{\geq 1}$. The positive divisors of p^a are $\{1, p, \ldots, p^a\}$, therefore $\tau(p^a) = a + 1$.

Now, let $k > 1$ be a positive integer. Thus $\tau(p^{k-1}) = k$, for any prime p. Since this holds for all primes, we conclude that $\tau(n) = k$ has infinitely many solutions.

Exercise 10. For any prime p and integer $d \geq 0$ we have $\tau(p^d) = |\{1, p, \ldots, p^d\}| = d + 1$.

Let $n \in \mathbb{Z}_{>0}$ and consider its prime factorization $n = p_1^{d_1} \cdots p_r^{d_r}$ where p_i are distinct primes, and arrange the primes so that $d_1 \geq d_2 \geq \cdots \geq d_r$.

Suppose $\tau(n) = 4$. As τ is multiplicative, we have

$$\tau(n) = (d_1 + 1) \cdots (d_r + 1) = 4$$

and, in particular, $d_1 + 1 \in \{4, 2, 1\}$, i.e. $d_1 = 3, 1$ or 0.

Suppose $d_1 = 3$; then $d_i + 1 = 1$ for $i \geq 2$. Thus $n = p_1^3$.

Suppose $d_1 = 1$; then $d_2 = 1$ and $d_i = 0$ for $i \geq 3$. Thus $n = p_1 p_2$.

Suppose $d_1 = 0$; then $d_2 > 0 = d_1$ which is impossible because we have $d_1 \geq d_2$.

We conclude that n has exactly four divisors if and only if $n = p^3$ for some prime p, or $n = p_1 p_2$ for distinct primes p_1, p_2.

Exercise 12. Let $k \in \mathbb{Z}_{>0}$ and suppose $n > 0$ is a solution to $\sigma(n) = k$.

As n and 1 are both divisors of n, we have $\sigma(n) \geq n + 1$. Thus $n + 1 \leq k$, that is, $n \leq k - 1$. We conclude there are most $k - 1$ solutions to $\sigma(n) = k$. In particular, there are only finitely many solutions, as desired.

Exercise 29. We have to prove both directions of the equivalence.

$\Rightarrow$: Suppose that $n > 0$ is composite. Then $n = ab$ for some integers a, b such that $1 < a, b < n$ and, without loss of generality, suppose $1 < a \le b < n$. Suppose that $a < \sqrt{n}$ and $b < \sqrt{n}$; then $n = ab < \sqrt{n}^2 = n$, a contradiction. We conclude that $b \ge \sqrt{n}$.

Therefore, n is divisble at least by the positive integers 1, b and n (note that we do not know if $b \ne a$), hence

$$\sigma(n) = \sum_{d|n, d>0} d \ge 1 + b + n \ge 1 + \sqrt{n} + n > n + \sqrt{n}.$$

$\Leftarrow$: We will prove the contrapositive. That is, if $n = 1$ or n is a prime then $\sigma(n) \le n + \sqrt{n}$.

If $n = 1$ then $\sigma(n) = 1 < 1 + \sqrt{1} = 2$, as desired.

Suppose that n is prime; thus $n > \sqrt{n} > 1$ and we compute

$$\sigma(n) = \sum_{d|n, d>0} d = 1 + n < n + \sqrt{n}.$$

Hence, if $\sigma(n) > n + \sqrt{n}$, necessarily, $n > 1$ is not prime, therefore n is composite.

Section 7.3

Exercise 1. By Theorem 7.10, n is an even perfect number if and only if

$$n = 2^{m-1}(2^m - 1),$$

where m is an integer such that $m \ge 2$ and $2^m - 1$ is prime. To determine whether $2^m - 1$ is prime, we use Theorem 7.11, which tells us that m must be prime if $2^m - 1$ is.

(1) Hence, taking $m = 2$, we get

$$n = 2^1(2^2 - 1) = 2 \cdot 3 = 6.$$

(Since 6 is small we can double-check that $\sigma(6) = 1 + 2 + 3 + 6 = 12$, as expected.)

(2) Taking $m = 3$,

$$n = 2^2(2^3 - 1) = 4 \cdot 7 = 28.$$

Again, note that $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$, hence 28 is also perfect.

(3) Since $m = 4$ is not prime, we know that $2^4 - 1$ cannot be prime, hence

$$n = 2^3(2^4 - 1) = 8 \cdot 15$$

is not perfect. Hence take $m = 5$,

$$n = 2^4(2^5 - 1) = 16 \cdot 31 = 496.$$

By Theorem 7.10, 496 is perfect.

(4) Similarly, since $m = 6$ is not prime, we know that $2^6 - 1$ cannot be prime, hence

$$n = 2^5(2^6 - 1) = 32 \cdot 63$$

is not perfect. Hence take $m = 7$,

$$n = 2^6(2^7 - 1) = 64 \cdot 127 = 8128.$$

By Theorem 7.10, 8128 is perfect.

(5) Take $m = 11$. Then $2^{11} - 1 = 23 \cdot 89$ is not prime, hence this will not lead us to a perfect number. Take instead $m = 13$. Then

$$n = 2^{12}(2^{13} - 1) = 4069 \cdot 8191 = 33550336.$$

By Theorem 7.10, 33550336 is perfect.

(6) Take $m = 17$. Then

$$n = 2^{16}(2^{17} - 1) = 65536 \cdot 131071 = 8589869056.$$

By Theorem 7.10, 8589869056 is perfect.

Exercise 8. Recall that $n \in \mathbb{Z}_{>0}$ is perfect if $\sigma(n) = 2n$ and we say it is defficient if $\sigma(n) < 2n$.

Let n be a positive integer such that $\sigma(n) \leq 2n$. That is, n is either deficient or perfect. Suppose $a \mid n$ and $1 \leq a < n$. To show that a must be deficient, we prove the contrapositive. That is, if a is not deficient, i.e.

$$\sigma(a) \geq 2a,$$

then n is neither deficient nor perfect, i.e.

$$\sigma(n) > 2n.$$

Indeed, suppose $\sigma(a) \geq 2a$. Then, since $a \mid n$, there exists $k \in \mathbb{Z}_{>0}$ such that $n = ak$. Then, if $c > 0$ divides a, we have $ck \mid ak$, so $ck \mid n$, and

$$\sigma(n) = \sum_{d \mid n, d>0} d > \sum_{c \mid a, c>0} ck = (\sum_{c \mid a, c>0} c)k = \sigma(a)k \geq (2a)k = 2n,$$

as desired.

Exercise 14. We wish to show that

$$\sigma(n) = \sigma(p^a q^b) = (1 + p + \cdots + p^a)(1 + q + \cdots + q^b) < 2n = 2p^a q^b,$$

for distinct odd primes p, q and positive integers a, b. Dividing by $p^a q^b$, this is equivalent to showing

$$\left(1 + \frac{1}{p} + \cdots + \frac{1}{p^a}\right)\left(1 + \frac{1}{q} + \cdots + \frac{1}{q^b}\right) < 2.$$

By the finite geometric sum, this is equivalent to

$$\frac{1 - p^{-(a+1)}}{1 - \frac{1}{p}} \cdot \frac{1 - q^{-(b+1)}}{1 - \frac{1}{q}} < 2.$$

We assume, without loss of generality, that $p < q$. As p and q are odd, we have $p \geq 3$ and $q \geq 5$, thus we have

$$\frac{1 - p^{-(a+1)}}{1 - \frac{1}{p}} \cdot \frac{1 - q^{-(b+1)}}{1 - \frac{1}{q}} < \frac{1}{1 - \frac{1}{p}} \cdot \frac{1}{1 - \frac{1}{q}} \leq \frac{1}{1 - \frac{1}{3}} \cdot \frac{1}{1 - \frac{1}{5}} = \frac{3}{2} \cdot \frac{5}{4} = \frac{15}{8} < 2.$$

SOLUTIONS TO PROBLEM SET 5

Section 9.1

Exercise 2. Recall that for $(a, m) = 1$ we have $\text{ord}_m a$ divides $\phi(m)$.

a) We have $\phi(11) = 10$ thus $\text{ord}_{11} 3 \in \{1, 2, 5, 10\}$. We check

$$3^1 \equiv 3 \pmod{11}, \quad 3^2 \equiv 9 \pmod{11}, \quad 3^5 \equiv 9 \cdot 27 \equiv 9 \cdot 5 \equiv 45 \equiv 1 \pmod{11}$$

Thus $\text{ord}_{11} 3 = 5$.

b) We have $\phi(17) = 16$ thus $\text{ord}_{17} 2 \in \{1, 2, 4, 8, 16\}$. We compute

$$2^2 \equiv 4 \pmod{17}, \quad 2^4 \equiv -1 \pmod{17}, \quad 2^8 \equiv (-1)^2 \equiv 1 \pmod{17}$$

Thus $\text{ord}_{17} 2 = 8$.

c) We have $\phi(21) = 2 \cdot 6 = 12$ thus $\text{ord}_{21} 10 \in \{1, 2, 3, 4, 6, 12\}$. We compute

$$10^2 \equiv 16 \pmod{21}, \quad 10^3 \equiv 13 \pmod{21}, \quad 10^4 \equiv (-5)^2 \equiv 4 \pmod{21}$$

and $10^6 \equiv 4 \cdot 16 \equiv 1 \pmod{21}$. Thus $\text{ord}_{21} 10 = 6$.

d) We have $\phi(25) = 20$, thus $\text{ord}_{25} 9 \in \{1, 2, 4, 5, 10, 20\}$. We compute

$$9^2 \equiv 81 \equiv 6 \pmod{25}, \quad 9^4 \equiv 36 \equiv 11 \pmod{25}, \quad 9^5 \equiv 99 \equiv -1 \pmod{25}.$$

Thus $\text{ord}_{25} 9 = 10$.

Exercise 6. Recall that a primitive root (PR) modulo m is an element r with maximal order, that is $\text{ord}_m r = \phi(m)$.

a) Note that $\phi(4) = 2$, so we are looking for an element r such that $r^2 \equiv 1 \pmod{4}$, while $r \not\equiv 1 \pmod{4}$. Taking $r = 3$, we observe that indeed $3 \not\equiv 1 \pmod{4}$ and $\phi(4) = 2$, so $r = 3$ is a PR modulo 4.

b) $r = 2$ is a PR mod 5, as $\phi(5) = 4$ and $2^4 = 16$ is the first power of 2 congruent to 1 mod 5.

c) $r = 3$ is a PR mod 10, as $\phi(10) = 4$, $3^2 = 9 \not\equiv 1 \pmod{10}$ and the possible orders are $\{1, 2, 4\}$.

d) Note that $\phi(13) = 12$, hence $\text{ord}_{13} a \in \{1, 2, 3, 4, 6, 12\}$ for all $a \in \mathbb{Z}$ such that $(a, 13) = 1$. For example, we compute

$$2^2 \equiv 4 \pmod{13}, \quad 2^3 \equiv 8 \pmod{13}, \quad 2^4 \equiv 3 \pmod{13}$$

and $2^6 \equiv 64 \equiv -1 \pmod{13}$. Thus $\text{ord}_{13} 2 = 12$, hence $r = 2$ is a PR mod 13.

e) Note that $\phi(14) = 6$, hence $\text{ord}_{14} a \in \{1, 2, 3, 6\}$ for all $a \in \mathbb{Z}$ such that $(a, 14) = 1$. For example, we compute

$$3^2 \equiv 9 \pmod{14}, \qquad 3^3 \equiv 27 \equiv -1 \pmod{14}$$

and so $\text{ord}_{14} 3 = 6$, that is $r = 3$ is a PR mod 14.

f) Note that $\phi(18) = 6$, hence $\operatorname{ord}_{18} a \in \{1,2,3,6\}$ for all $a \in \mathbb{Z}$ such that $(a,18) = 1$. For example, we compute

$$5^2 \equiv 7 \pmod{18}, \qquad 5^3 \equiv 35 \equiv -1 \pmod{18}$$

and so $\operatorname{ord}_{18} 5 = 6$, that is $r = 5$ is a PR mod 18.

Exercise 8. We have $\phi(20) = \phi(4)\phi(5) = 8$, hence $\operatorname{ord}_{20}(a) \in \{1,2,4,8\}$ for all $a \in \mathbb{Z}$ such that $(a,20) = 1$. To prove there are no primitive roots mod 20 we have to show that $\operatorname{ord}_{20}(a) = 8$ never occurs.

It suffices to show that for all a such that $0 \le a \le 19$ and $(a,20) = 1$ we have $a^d \equiv 1 \pmod{20}$ for some $d \in \{1,2,4\}$. Indeed, all such values of a are $\{1,3,7,9,11,13,17,19\}$. Clearly, $1^1 \equiv 1 \pmod{20}$ and direct calculations show that

$$9^2 \equiv 11^2 \equiv 19^2 \equiv 1 \pmod{20} \quad \text{and} \quad 3^4 \equiv 7^4 \equiv 13^4 \equiv 17^4 \equiv 1 \pmod{20}.$$

Exercise 12. Let $a,b,n \in \mathbb{Z}$ satisfy $n > 0$, $(a,n) = (b,n) = 1$ and $(\operatorname{ord}_n a, \operatorname{ord}_n b) = 1$.

Write $y = \operatorname{ord}_n a \cdot \operatorname{ord}_n b$. We have

$$(ab)^y = a^y b^y = (a^{\operatorname{ord}_n a})^{\operatorname{ord}_n b}(b^{\operatorname{ord}_n b})^{\operatorname{ord}_n a} \equiv 1 \cdot 1 \equiv 1 \pmod{n},$$

hence $\operatorname{ord}_n(ab) \mid y$. Therefore $\operatorname{ord}_n(ab) \le \operatorname{ord}_n a \cdot \operatorname{ord}_n b$.

To finish the proof, we will now show the opposite inequality $\operatorname{ord}_n(ab) \ge \operatorname{ord}_n a \cdot \operatorname{ord}_n b$.

Note that $(b,n) = 1$ implies b has an inverse b^{-1} modulo n. Furthermore, for $k \ge 0$ we have $(b^k, n) = 1$ and the inverse of b^k is $(b^{-1})^k$ which is usually denoted b^{-k}. Suppose $(ab)^x \equiv 1 \pmod{n}$, which is equivalent to $a^x \equiv b^{-x} \pmod{n}$, because b^{-1} exists. We now compute

$$a^{x \cdot \operatorname{ord}_n b} = (a^x)^{\operatorname{ord}_n b} \equiv (b^{-x})^{\operatorname{ord}_n b} \equiv (b^{-1})^{x \operatorname{ord}_n b} \equiv (b^{x \operatorname{ord}_n b})^{-1} \equiv ((b^{\operatorname{ord}_n b})^x)^{-1} \equiv 1 \pmod{n},$$

hence $\operatorname{ord}_n a \mid x \cdot \operatorname{ord}_n b$. Since $(\operatorname{ord}_n a, \operatorname{ord}_n b) = 1$ we have $\operatorname{ord}_n a \mid x$.

Note that the argument in the previous paragraph also holds if we swap a and b, so we also have $\operatorname{ord}_n b \mid x$.

We have just shown that $(ab)^x \equiv 1 \pmod{n}$ implies $\operatorname{ord}_n a \cdot \operatorname{ord}_n b \mid x$. In particular, taking $x = \operatorname{ord}_n(ab)$ implies $\operatorname{ord}_n(ab) \ge \operatorname{ord}_n a \cdot \operatorname{ord}_n b$, as desired.

We conclude $\operatorname{ord}_n(ab) = \operatorname{ord}_n a \cdot \operatorname{ord}_n b$.

Exercise 16. For $m = 1$ we have $\operatorname{ord}_m a = 1 - 1 = 0$ which makes no sense, so $m > 1$.

Suppose $m > 1$. By definition $\phi(m)$ is the number of integers a in the interval $1 \le a \le m$ satisfying $(a,m) = 1$. In particular, it follows that $1 \le \phi(m) \le m - 1$, because $(m,m) = m > 1$.

Let $a, m \in \mathbb{Z}$ satisfy $m > 1$ and $(a,m) = 1$. We know that $\operatorname{ord}_m a \mid \phi(m)$.

Suppose $\operatorname{ord}_m a = m - 1$; then $\phi(m) \ge m - 1$. We conclude $\phi(m) = m - 1$. This can only occur if m is prime, finishing the proof. Indeed, suppose m is composite hence it has some factor n in the interval $1 < n < m - 1$. Clearly, $(n,m) = n \ne 1$ therefore $\phi(m)$ is at most $m - 2$.

Exercise 5. We know that there are $\phi(\phi(13)) = \phi(12) = 4$ incongruent primitive roots mod 13. For each k in $1 \le k \le 12$ we have $(k, 13) = 1$ and we compute $k^i \pmod{13}$ for all $i > 0$ dividing $\phi(13) = 12$, that is $i \in \{1, 2, 3, 4, 6, 12\}$.

From FLT we know that $k^{12} \equiv 1 \pmod{13}$, so the primitive roots are the values of k such that $k^i \not\equiv 1 \pmod{13}$ for all $i \in \{1, 2, 3, 4, 6\}$. We stop when we find four such values of k; these are $\{2, 6, 7, 11\}$.

Alternative proof requiring less computations. Computing $2^i \pmod{13}$ for i a positive divisor of $\phi(13) = 12$, that is $i \in \{1, 2, 3, 4, 6, 12\}$ (the possible orders of 2 modulo 13) we verify that $2^i \not\equiv 1 \pmod{13}$ for all $i \in \{1, 2, 3, 4, 6\}$, hence 2 has order 12, so it is a primitive root mod 13. Thus $\{2^i\}$, $1 \le i \le 12$ forms a reduced residue system. We also know that

$$\operatorname{ord}_{13} 2^i = \frac{\operatorname{ord}_{13} 2}{(i, \operatorname{ord}_{13} 2)}.$$

Now, if $\operatorname{ord}_{13} 2^i = 12$ then $(i, \operatorname{ord}_{13} 2) = (i, 12) = 1$ which occurs exactly when $i = 1, 5, 7, 11$. Therefore, 2, 2^5, 2^7 and 2^{11} are four non-congruent primitive roots modulo 13.

If we want to obtain the smallest representatives for each of these primitive roots we have to reduce them modulo 13, obtaining

$$2^1 \equiv 2, \quad 2^5 \equiv 6, \quad 2^7 \equiv 11, \quad 2^{11} \equiv 7 \pmod{13}$$

to conclude that $\{2, 6, 7, 11\}$ is a set of all incongruent primitive roots mod 13 with smallest possible representatives, which was expected by our previous solution.

Exercise 8. Let r be a primitive root mod p, that is $\operatorname{ord}_p r = \phi(p) = p - 1$.

We first show that $r^{\frac{p-1}{2}} \equiv -1 \mod p$. Indeed, denote $r^{\frac{p-1}{2}}$ by x; then $x^2 \equiv r^{p-1} \equiv 1 \mod p$. Hence $x \equiv 1$ or $-1 \mod p$. But $x = r^{\frac{p-1}{2}}$ cannot be $1 \mod p$, because it would contradict $\operatorname{ord}_p r = p - 1$. Hence $x \equiv -1 \mod p$ as claimed.

Now we want to show that $-r$ is a primitive root, that is $\operatorname{ord}_p(-r) = p - 1$.

We have that

$$-r \equiv (-1)r \equiv r^{\frac{p-1}{2}+1} \pmod{p},$$

where in the second congruence we used that $r^{\frac{p-1}{2}} \equiv -1 \mod p$. We will determine the order of $r^{\frac{p-1}{2}+1} \mod p$ by using the formula

$$\operatorname{ord}_p r^k = \frac{\operatorname{ord}_p r}{(\operatorname{ord}_p r, k)}.$$

Taking $k = \frac{p-1}{2} + 1$ and since $\operatorname{ord}_p r = p - 1$ we have to show that $(p - 1, \frac{p-1}{2} + 1) = 1$.

We note that up to this point we have not yet used the hypothesis $p \equiv 1 \pmod{4}$.

From $p \equiv 1 \pmod{4}$, we can write p as $4m + 1$ for some integer $m \ge 1$. Then $p - 1 = 4m$, and $\frac{p-1}{2} + 1 = 2m + 1$. Thus we want to prove that $(4m, 2m + 1) = 1$ for any integer $m \ge 1$.

Recall that for all $a, b, q \in \mathbb{Z}$ with $a \ge b > 0$ we have $(a, b) = (b, a - bq)$. This gives

$$(4m, 2m + 1) = (2m + 1, 4m - 2(2m + 1)) = (2m + 1, -2) = (2m + 1, 2) = 1,$$

as desired. In summary, $\mathrm{ord}_p(-r) = \mathrm{ord}_p(r^{2m+1}) = \frac{p-1}{\gcd(4m,2m+1)} = \frac{p-1}{1} = p-1$, that is $-r$ is a primitive root.

Exercise 10.

a)

$x^2 - x$ has 4 incongruent solutions mod 6, namely, $0, 1, 3$, and 4. Indeed, modulo 6 we have

$$0^2 - 0 \equiv 0, \quad 1^2 - 1 \equiv 0, \quad 2^2 - 2 \equiv 2 \not\equiv 0 \pmod{6},$$

$$3^2 - 3 \equiv 3 - 3 \equiv 0, \quad 4^2 - 4 \equiv 4 - 4 \equiv 0, \quad \text{and} \quad 5^2 - 5 \equiv 2 \not\equiv 0 \pmod{6}.$$

b)

Part (a) does not violate Lagrange's theorem because the modulus in Lagrange's theorem must be prime, but the modulus in part a) is composite.

Exercise 16. Let p be a prime of the form $p = 2q + 1$, where q is an odd prime.

Let $a \in \mathbb{Z}$ satisfy $1 < a < p - 1$; in particular, $(a, p) = 1$. Since $p - a^2 \equiv -a^2 \pmod{p}$ we have $\mathrm{ord}_p(p - a^2) = \mathrm{ord}_p(-a^2)$. We will show that $\mathrm{ord}_p(-a^2) = p - 1$.

We know that $\mathrm{ord}_p(-a^2)$ divides $\phi(p) = p - 1 = 2q$. Thus $\mathrm{ord}_p(-a^2) = 1, 2, q$, or $2q$. We have to rule out $1, 2$ and q. Equivalently, we need to show that

(1) $(-a^2)^2 \not\equiv 1 \pmod{p}$
(2) $(-a^2)^q \not\equiv 1 \pmod{p}$

Proof of (1): Assume the contrary. Then, $a^4 \equiv 1 \pmod{p}$. Thus $\mathrm{ord}_p a$ divides both 4 and $p - 1 = 2q$. Hence, $\mathrm{ord}_p a$ divides $\gcd(4, 2q) = 2$. In particular, $a^2 \equiv 1 \pmod{p}$, therefore $a \equiv \pm 1 \pmod{p}$. This contradicts $1 < a < p - 1$, completing the proof of (1).

Proof of (2): Assume the contrary, that is $(-a^2)^q \equiv 1 \pmod{p}$. Therefore,

$$1 \equiv (-a^2)^q \equiv (-1)^q a^{2q} \equiv (-1)^q \equiv -1 \pmod{p},$$

where in the 3rd congruence we applied FLT and in the last one we used the fact that q is odd. Thus, $-1 \equiv 1 \pmod{p}$, a contradiction since $p > 2$.

Section 9.4

Exercise 2. We first note that 5 is a primitive root of 23.

To solve this problem consult the table of indexes relative to 5 modulo 23. It is given as the answer to problem 1 of Section 9.4.

a) We want to solve $3x^5 \equiv 1 \pmod{23}$.

Taking the index of both sides of our equation, gives

$$\mathrm{ind}_5(3x^5) \equiv \mathrm{ind}_5(1) \equiv 0 \pmod{\phi(23) = 22}$$

which expands into

$$\mathrm{ind}_5(3) + 5\,\mathrm{ind}_5(x) \equiv 0 \pmod{22} \quad \Leftrightarrow \quad 5\,\mathrm{ind}_5(x) \equiv -16 \equiv 6 \pmod{22}.$$

Since $5^{-1} \equiv 9 \pmod{22}$ we get $\text{ind}_5(x) \equiv 10 \pmod{22}$ which means that $x \equiv 9 \pmod{23}$.

b) We want to solve $3x^{14} \equiv 2 \pmod{23}$. The procedure is similar as before.

Take the index of both sides of our equation, giving $\text{ind}_5(3x^{14}) \equiv \text{ind}_5(2) \equiv 2 \pmod{22}$. Now, we expand this into $\text{ind}_5(3) + 14\,\text{ind}_5(x) \equiv 2 \pmod{22}$. Hence, $14\,\text{ind}_5(x) \equiv -14 \equiv 8 \pmod{22}$. We then reduce this equation on all sides by 2, giving us $7\,\text{ind}_5(x) \equiv 4 \pmod{11}$.

Since $7^{-1} \equiv 8 \pmod{11}$ we obtain $\text{ind}_5(x) \equiv 10 \pmod{11}$. Therefore, $\text{ind}_5(x) \equiv 10, 21 \pmod{22}$. Using the table of indices, we find that this means that $x \equiv 9, 14 \pmod{23}$.

Exercise 3.

a) We want to solve $3^x \equiv 2 \pmod{23}$.

We know 5 is a primitive root mod 23. Note that $\phi(23) = 22$. We take the index of both sides giving

$$x\,\text{ind}_5(3) \equiv 2 \pmod{22} \quad \Leftrightarrow \quad 16x \equiv 2 \pmod{22}.$$

Thus $8x \equiv 1 \pmod{11}$ and since $8^{-1} \equiv 7 \pmod{11}$ we have $x \equiv 7 \pmod{11}$.

Thus, $x \equiv 7, 18 \pmod{22}$.

b) We want to solve $13^x \equiv 5 \pmod{23}$.

If there is such an x, taking the index of both sides we obtain $x\,\text{ind}_5(13) \equiv 1 \pmod{22}$, or rather, $14x \equiv 1 \pmod{22}$, which means that 14 is invertible mod 22. But since $(14, 22) = 2$ we know that 14 is not invertible mod 22; thus the initial equation cannot have solutions.

Exercise 4. Consider the equation $ax^4 \equiv 2 \pmod{13}$.

We check that 2 is a primitive root mod 13. Taking the index of both sides we have $\text{ind}_2(a) + 4\,\text{ind}_2(x) \equiv 1 \pmod{12}$, or rather, $4\,\text{ind}_2(x) \equiv 1 - \text{ind}_2(a) \pmod{12}$.

Write $y = \text{ind}_2(x)$. Thus, the above gives the linear congruence

$$4y \equiv 1 - \text{ind}_2(a) \pmod{12}$$

which, since $\gcd(4, 12) = 4$, will have a solution if and only if $4 \mid 1 - \text{ind}_2(a)$. This will be the case only when $\text{ind}_2(a) \equiv 1, 5, 9 \pmod{12}$, which correspond to $a \equiv 2, 6, 5 \pmod{13}$.

Alternative proof: If $13 \mid a$ then clearly there are no solutions. Suppose $13 \nmid a$. Thus a^{-1} mod 13 exists and we multiply the congruence by it to obtain $x^4 \equiv 2a^{-1} \pmod{13}$. Write $d = (4, \phi(13)) = (4, 12) = 4$. Thus, we have seen in class that $x^4 \equiv 2a^{-1} \pmod{13}$ will have solutions if and only if $(2a^{-1})^{\phi(13)/d} \equiv 1 \pmod{13}$. This is equivalent to $a^3 \equiv 8 \pmod{13}$. Direct computations show this holds exactly when $a \equiv 2, 5, 6 \pmod{13}$, as expected.

Exercise 5. Consider the equation $8x^7 \equiv b \pmod{29}$.

We check that 2 is a primitive root mod 29.

If $b \equiv 0 \pmod{29}$ then the equation has the solution of $x \equiv 0 \pmod{29}$.

Suppose that $b \not\equiv 0 \mod 29$. Taking the index gives $\text{ind}_2(8) + 7\,\text{ind}_2(x) \equiv \text{ind}_2(b) \pmod{28}$, or rather, $7\,\text{ind}_2(x) \equiv \text{ind}_2(b) - 3 \pmod{28}$.

Write $y = \text{ind}_2(x)$. The previous gives the linear congruence

$$7y \equiv \text{ind}_2(b) - 3 \pmod{28},$$

which, since $\gcd(7,28) = 7$, will have a solution if and only if $7 \mid \operatorname{ind}_2(b) - 3$. This is the case when $\operatorname{ind}_2(b) \equiv 3, 10, 17, 24 \pmod{28}$, which correspond to $b \equiv 8, 9, 20, 21 \pmod{29}$.

We conclude that the complete list of values of b such that the initial equation has solutions is $b \equiv 0, 8, 9, 20, 21 \pmod{29}$.

Alternative proof for the case $b \not\equiv 0 \pmod{29}$: Multiply the congruence by 8^{-1} mod 29 obtaining $x^7 \equiv 8^{-1}b \pmod{29}$. Write $d = (7, \phi(29)) = (7, 28) = 7$. Thus, we have seen in class that $x^7 \equiv 8^{-1}b \pmod{29}$ will have solutions if and only if $(8^{-1}b)^{\phi(29)/d} \equiv 1 \pmod{29}$. This is equivalent to $b^4 \equiv 7 \pmod{29}$. Direct computations show this holds exactly when $b \equiv 8, 9, 20, 21 \pmod{29}$.

Exercise 8. Let p be an odd prime and r a primitive root mod p, that is $\operatorname{ord}_p r = \phi(p) = p-1$.

Note that $p - 1 \equiv -1 \pmod{p}$. Thus we have to show that

$$r^{\frac{p-1}{2}} \equiv -1 \pmod{p} \quad \text{and} \quad r^i \not\equiv -1 \pmod{p} \ \text{ for } \ 1 \le i < (p-1)/2.$$

Since p is odd, $p-1$ is even and $(r^{\frac{p-1}{2}})^2 = r^{p-1} \equiv 1 \pmod{p}$; thus $r^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. If $r^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ then $\operatorname{ord}_p r < p-1$, a contradiction. We conclude $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Suppose that $r^i \equiv -1 \pmod{p}$ for some $i < (p-1)/2$; therefore $(r^i)^2 = r^{2i} \equiv 1 \pmod{p}$ and $2i < 2(p-1)/2 = p-1$, which again means $\operatorname{ord}_p r < p-1$, a contradiction.

Exercise 9. Let p be an odd prime. We have $\phi(p) = p-1$ is even.

Write $d = (4, p-1)$. From class or Theorem 9.17 in Rosen, we know that $x^4 \equiv -1 \pmod{p}$ has a solution if and only if $(-1)^{\frac{\phi(p)}{d}} \equiv 1 \pmod{p}$. Since the order of -1 mod p is 2 we must have $2 \mid \frac{p-1}{d}$. That is, there exists k such that $2k = \frac{p-1}{(p-1,4)}$.

Since $p-1$ is even we have $(p-1, 4) = 2$ or 4. If $(p-1, 4) = 2$ then $\frac{p-1}{(p-1,4)}$ must be odd, a contradiction. Therefore, $(p-1, 4) = 4$, so $2k = \frac{p-1}{4}$, or rather, $8k + 1 = p$, as required.

Exercise 18. An integer a is called a cubic residue mod p when there is an integer r such that $r^3 \equiv a \pmod{p}$. In other words, the congruence equation $x^3 \equiv a \pmod{p}$ has a solution.

Let $p > 3$ be a prime and a an integer not divisible by p. We want to know if the congruence $x^3 \equiv a \pmod{p}$ has a solution, where a is fixed and we are solving for x.

Note that $(a, p) = 1$ and let $d = \gcd(3, p-1)$.

By Theorem 9.17 in Rosen a solution exists if and only if $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$.

(1) Suppose $p \equiv 2 \pmod{3}$. Then $d = 1$ and $a^{\frac{p-1}{d}} \equiv a^{p-1} \equiv 1 \pmod{p}$ by FLT.

(2) Suppose $p \equiv 1 \pmod{3}$. Then $d = 3$ and a solution exists if and only if $a^{\frac{p-1}{3}} \equiv 1 \pmod{p}$.

Why is $d = 1$ in part (1) and $d = 3$ in part (2)?

Since the only divisors of 3 are 1 and 3 it follows that $d = 1$ if $3 \nmid p-1$ and $d = 3$ if $3 \mid p-1$.

In part (1) we have $p - 1 \equiv 1 \pmod{3}$ so $p-1$ is not divisible by 3. In part (2) we have $p - 1 \equiv 0 \pmod{3}$ so $p-1$ is divisible by 3.

SOLUTIONS TO PROBLEM SET 6

Section 3.6

Exercise 4.

b)

(i) We have $\sqrt{73} \approx 8.5$, so $t = 9$ is the smallest integer $\geq \sqrt{73}$;

(ii) We calculate

$$9^2 - 73 = 8$$
$$10^2 - 73 = 27$$
$$11^2 - 73 = 48$$
$$12^2 - 73 = 71$$
$$13^2 - 73 = 96$$
$$14^2 - 73 = 123$$
$$15^2 - 73 = 152$$
$$16^2 - 73 = 183$$
$$17^2 - 73 = 216$$
$$18^2 - 73 = 251$$
$$19^2 - 73 = 288$$
$$20^2 - 73 = 327$$
$$21^2 - 73 = 368$$
$$22^2 - 73 = 411$$
$$23^2 - 73 = 456$$
$$24^2 - 73 = 503$$
$$25^2 - 73 = 552$$
$$26^2 - 73 = 603$$
$$27^2 - 73 = 656$$
$$28^2 - 73 = 711$$
$$29^2 - 73 = 768$$
$$30^2 - 73 = 827$$
$$31^2 - 73 = 888$$
$$32^2 - 73 = 951$$

$$\begin{aligned}
33^2 - 73 &= 1016\\
34^2 - 73 &= 1083\\
35^2 - 73 &= 1152\\
36^2 - 73 &= 1223\\
37^2 - 73 &= 1296 = 36^2
\end{aligned}$$

(iii) Thus we have that $73 = 37^2 - 36^2 = (37-36)(37+36) = 1 \cdot 73$ is the only factorization of 73, hence 73 is prime.

c)

(i) We have $\sqrt{46009} \approx 214.5$, so $t = 215$ is the smallest integer $\geq \sqrt{46009}$.

(ii) We calculate

$$\begin{aligned}
215^2 - 46009 &= 216\\
216^2 - 46009 &= 647\\
217^2 - 46009 &= 1080\\
218^2 - 46009 &= 1515\\
219^2 - 46009 &= 1952\\
220^2 - 46009 &= 2391\\
221^2 - 46009 &= 2832\\
222^2 - 46009 &= 3275\\
223^2 - 46009 &= 3720\\
224^2 - 46009 &= 4167\\
225^2 - 46009 &= 4616\\
226^2 - 46009 &= 5067\\
227^2 - 46009 &= 5520\\
228^2 - 46009 &= 5975\\
229^2 - 46009 &= 6432\\
230^2 - 46009 &= 6891\\
231^2 - 46009 &= 7352\\
232^2 - 46009 &= 7815\\
233^2 - 46009 &= 8280\\
234^2 - 46009 &= 8747\\
235^2 - 46009 &= 9216 = 96^2;
\end{aligned}$$

(iii) Thus $46009 = 235^2 - 96^2 = (235-96)(235+96) = 139 \cdot 331$ is a factorization. Since the two factors are primes we conclude this is the prime factorization.

d)

(i) We have $\sqrt{11021} \approx 104.98$, so $t = 105$ is the smallest integer $\geq \sqrt{11021}$;

(ii) We calculate $105^2 - 11021 = 4 = 2^2$;

(iii) Thus we have that $11021 = 105^2 - 2^2 = (105-2)(105+2) = 103 \cdot 107$ is a factorization. Since the two factors are prime it is the prime factorization.

Section 6.1

Exercise 27. Let $R_k \equiv 2^{k!} \pmod{7331117}$ for $k \in \mathbb{Z}_{>0}$. We have $R_{k+1} \equiv R_k^{k+1} \pmod{7331117}$. We successively compute R_k and $(R_k-1, 7331117)$ until the latter is different from 1, in which case we have found a divisor of $7,331,117$. Indeed,

$$
\begin{array}{lcll}
R_1 & = & 2^1 \equiv 2 \pmod{7331117}, & (1, 7331117) = 1 \\
R_2 & = & 2^2 \equiv 4 \pmod{7331117}, & (3, 7331117) = 1 \\
R_3 & = & 4^3 \equiv 64 \pmod{7331117}, & (63, 7331117) = 1 \\
R_4 & = & 64^4 \equiv 2114982 \pmod{7331117}, & (2114981, 7331117) = 1 \\
R_5 & = & 2114982^5 \equiv 2937380 \pmod{7331117}, & (2937379, 7331117) = 1 \\
R_6 & = & 2937380^6 \equiv 6924877 \pmod{7331117}, & (6924876, 7331117) = 1 \\
R_7 & = & 6924877^7 \equiv 3828539 \pmod{7331117}, & (3828538, 7331117) = 1 \\
R_8 & = & 3828539^8 \equiv 4446618 \pmod{7331117}, & (4446617, 7331117) = 641
\end{array}
$$

Thus $641 \mid 7331117$.

Section 8.1

Exercise 2. The Caeser cipher uses the encryption function $E(x) = x + 3 \pmod{26}$ whose corresponding decryption function is $D(x) = x - 3 \pmod{26}$. We apply D to the numerical values of the letters to obtain the message

I CAME I SAW I CONQUERED.

Exercise 6. We know that the decryption function corresponding to the affine encryption function $E(x) = 3x + 24$ is given by

$$D(y) = cy + d \pmod{26}, \quad \text{where} \quad c = 3^{-1} \equiv 9, \quad d \equiv -9 \cdot 24 \equiv 18.$$

Using D to decrypt the message we obtain PHONE HOME.

Problem 8. The most commonly occurring letter in the ciphertext is V (8 occurrences) which has numerical value of 21. It is reasonable to guess this is the image of E, the most common letter in English. The numerical value of E is 4, therefore, the decryption function $D(y) = y - k$ must satisfy

$$D(21) = 21 - k \equiv 4 \pmod{26},$$

that is $k = 17$. Using D to decode the ciphertext gives

THE VALUE OF THE KEY IS SEVENTEEN.

Exercise 10. The most common letters in English are E and T (in this order), therefore it is reasonable to assume that E is encrypted as X and T is encrypted as Q. In terms of the affine encryption function $E(x) = ax + b \pmod{26}$ this gives rise to the congruences

$$4a + b \equiv 23 \pmod{26} \qquad \text{and} \qquad 19a + b \equiv 16 \pmod{26}.$$

Subtracting the first congruence from the second gives $15a \equiv -7 \pmod{26}$, hence $a \equiv 3 \pmod{26}$. Then $b \equiv 23 - 12 \equiv 11 \pmod{26}$.

Thus the most likely values for a and b are $a = 3$ and $b = 11$.

Exercise 12. The two most frequent letters in the cipher text are M (7 occurrences) and R (6 occurrences). We guess these correspond to E and T. In terms of the affine transformation $E(x) = ax + b \pmod{26}$ we get

$$4a + b \equiv 12 \pmod{26} \qquad \text{and} \qquad 19a + b \equiv 17 \pmod{26}.$$

Subtracting the first congruence from the second gives $15a \equiv 5 \pmod{26}$. As $(5, 26) = 1$, this is equivalent to $3a \equiv 1 \pmod{26}$, which gives $a \equiv 9 \pmod{26}$.

Thus $b \equiv 12 - 36 \equiv 2 \pmod{26}$. Then the encryption becomes $E(x) = 9x + 2 \pmod{26}$ and its corresponding decryption function is

$$D(y) = a^{-1}y - a^{-1}b = 3y - 6 \pmod{26}.$$

Using this the message decodes to

EVERY ALCHEMIST OF ANCIENT TIMES KNEW HOW TO TURN LEAD INTO GOLD.

Section 8.3

Exercise 6. The encryption function is $E(x) = x^e \pmod{p = 29}$, where e is the encryption key which satisfies $(p - 1, e) = (28, e) = 1$. We know that

$$E(20) \equiv 24 \pmod{29} \quad \Leftrightarrow \quad 20^e \equiv 24 \pmod{29}.$$

We calculate

$$20^2 \equiv 400 \equiv -6 \pmod{29},$$
$$20^4 \equiv 36 \equiv 7 \pmod{29},$$
$$20^8 \equiv 49 \equiv 20 \pmod{29},$$

which shows that $20^7 \equiv 1 \pmod{29}$. Dividing e by 7 with the division algorithm gives

$$e = 7k + e', \qquad 0 \le e' \le 6;$$

therefore

$$20^e \equiv 20^{7k+e'} \equiv 20^{7k} \cdot 20^{e'} \equiv 20^{e'} \equiv 24 \pmod{29}.$$

We continue calculating

$$20^3 \equiv 54 \equiv 25 \equiv -4 \pmod{29},$$
$$20^5 \equiv 20^2 \cdot 20^3 \equiv (-6) \cdot (-4) \equiv 24 \pmod{29}$$

to find that $e' = 5$. We guess that our encryption key is $e = e' = 5$ (i.e. $k = 0$). To find the corresponding decryption key d we need to solve $5d \equiv 1 \pmod{\phi(29) = 28}$. We obtain $d = 17$

as a solution. The decryption function is $D(y) = y^{17} \pmod{29}$ and the decoded message would become

$$061414030620041818$$

which corresponds to

GOOD GUESS.

Section 8.4

Exercise 2. Recall that for a quadratic polynomial $ax^2 + bx + c$ its two roots are given by the quadratic resolvent formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

We note that

$$\phi(n) = \phi(pq) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$$

and so

$$-(p+q) = \phi(n) - n - 1.$$

Note that p and q are roots of the quadratic polynomial $P(x) = (x-p)(x-q)$, which becomes

$$P(x) = x^2 - (p+q)x + pq = x^2 + (\phi(n) - n - 1)x + n.$$

In our case, $n = 4386607$ and $\phi(n) = 4382136$ and this becomes

$$P(X) = x^2 + (4382136 - 4386607 - 1)x + 4386607 = x^2 - 4472x + 4386607.$$

Using the resolvent formula, we find the roots p and q of $P(x)$ to be

$$x = \frac{4472 \pm \sqrt{4472^2 - 4 \cdot 1 \cdot 4386607}}{2} = 1453 \quad \text{and} \quad 3019.$$

Exercise 8. The encryption key is $(e, n) = (5, 2881)$.

We have $2881 = 43 \cdot 67$. Thus $\phi(n) = 42 \cdot 66 = 2772$. Using the Euclidean Algorithm, we compute the decryption key, $d \equiv e^{-1} \pmod{2772}$. This gives $d \equiv 1109 \pmod{2772}$. To decrypt the message, we raise each block in

0504 1874 0347 0515 2088 2356 0736 0468

to the power of 1109 and reduce modulo 2881. This gives us

0400 1902 0714 0214 1100 1904 0200 1004

or EAT CHOCOLATE CAKE.

Exercise 14. Let the moduli be n_1, n_2, n_3 and write $n_1 = p_1q_1$, $n_2 = p_2q_2$ and $n_3 = p_3q_3$, with p_i, q_i all prime and $p_i \neq q_i$ for fixed i.

First, using Euclidean Algorithm, we compute $\gcd(n_1, n_2)$, $\gcd(n_2, n_3)$, and $\gcd(n_1, n_3)$. If one of these numbers is not 1, say $\gcd(n_1, n_2) \neq 1$, then n_1 and n_2 have a prime factor in common, say $p_1 = p_2$. Then $\gcd(n_1, n_2) = p_1$ and we have factored n_1, thus breaking the code. Thus can assume $\gcd(n_1, n_2) = \gcd(n_1, n_3) = \gcd(n_2, n_3) = 1$, that is, the moduli n_1, n_2 and n_3 are pairwise coprime.

We know that each encryption function is $E_i(x) = x^3 \pmod{n_i}$ and from a plaintext message P we intercepted the three ciphertext messages C_i that satisfy $0 \le C_i < n_i$ and

$$P^3 \equiv C_1 \pmod{n_1}, \quad P^3 \equiv C_2 \pmod{n_2}, \quad P^3 \equiv C_3 \pmod{n_3}.$$

This means that the system of congruences

$$x \equiv C_1 \pmod{n_1}, \quad x \equiv C_2 \pmod{n_2}, \quad x \equiv C_3 \pmod{n_3}$$

has the solution P^3. On the other hand, by the CRT, there is a unique solution C to

$$C \equiv C_i \pmod{n_i}, \quad \text{satisfying} \quad 0 \le C \le n_1 n_2 n_3 - 1.$$

Now, P satisfies $0 \le P \le \min\{n_1, n_2, n_3\} - 1$, and so P^3 is an integer satisfying

$$0 \le P^3 \le (\min\{n_1, n_2, n_3\} - 1)^3 < n_1 n_2 n_3 - 1,$$

therefore $C = P^3$. We can apply CRT recipe to determine $P^3 = C$ from the C_i and n_i and then recover P by taking the cube root.

Exercise 16. Write $n_i = p_i q_i$ and suppose $n_1 \ne n_2$. If $(n_1, n_2) > 1$ then $1 < (n_1, n_2) < n_1$ and we can factor n_1 as $n_1 = (n_1, n_2) \cdot \frac{n_1}{(n_1, n_2)}$. Thus the two factors in this factorization correspond in some order to p_1 and q_1. This allows to calculate $\phi(n) = (p_1 - 1)(q_1 - 1)$ and find $d \equiv e^{-1}$ mod $\phi(n)$, breaking the system.

SOLUTIONS TO PROBLEM SET 7

Section 13.1

Exercise 2. Note that for any integer a we have $a^2 \equiv 0, 1 \pmod 3$, because

$$0^2 \equiv 0 \pmod 3, \quad 1^2 \equiv 1 \pmod 3, \quad 2^2 = 4 \equiv 1 \pmod 3.$$

Let $x, y, z \in \mathbb{Z}_{>0}$ form a PPT, that is $(x, y, z) = 1$ and $x^2 + y^2 = z^2$.

From the above $x^2 + y^2 \equiv z^2 \equiv 0, 1 \pmod 3$, which implies that least one of x^2 or y^2 is congruent to 0 modulo 3. WLOG we can assume $x^2 \equiv 0 \pmod 3$.

Therefore $x^2 = x \cdot x = 3k$ for some integer $k \neq 0$. Since 3 is a prime we conclude that $3 \mid x$.

Suppose we also have $y^2 \equiv 0 \pmod 3$. Then, the same argument leads to $3 \mid y$. Thus $3 \mid x^2 + y^2 = z^2$, hence $3 \mid z$ which contradicts $(x, y, z) = 1$. We conclude that $3 \nmid y$, as desired.

Exercise 3. Note that for an integer a we have $a^2 \equiv 0, \pm 1 \pmod 5$, because

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 = 4 \equiv -1, \quad 3^2 = 9 \equiv -1, \quad 4^2 = 16 \equiv 1 \pmod 5.$$

Let $x, y, z \in \mathbb{Z}_{>0}$ form a PPT, that is $(x, y, z) = 1$ and $x^2 + y^2 = z^2$.

From class or Lemma 13.1 in Rosen we have $(x, y) = (y, z) = (x, z) = 1$, therefore 5 divides at most one of x, y, z, so if $5 \mid x$ or $5 \mid y$ the result follows.

To finish the proof, we assume that $5 \nmid x$ and $5 \nmid y$ and will show that $5 \mid z$. Indeed, from the calculations above it follows $x^2 \equiv \pm 1 \pmod 5$ and $y^2 \equiv \pm 1 \pmod 5$, therefore

$$z^2 \equiv x^2 + y^2 \equiv 0, 2, -2 \pmod 5.$$

Since we have $a^2 \not\equiv \pm 2 \pmod 5$ for all $a \in \mathbb{Z}$, we conclude $z^2 \equiv 0 \pmod 5$. Therefore, $z^2 = z \cdot z = 5k$ for some integer $k \neq 0$ and since 5 is a prime it follows that $5 \mid z$, as desired.

Exercise 4. Note that for an integer a we have $a^2 \equiv 0, 1 \pmod 4$, because

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 = 4 \equiv 0, \quad 3^2 = 9 \equiv 1 \pmod 4.$$

Furthermore, we have $a^2 \equiv 0 \pmod 4$ if and only if a is even; and $a^2 \equiv 1 \pmod 4$ if and only if a is odd.

Let $x, y, z \in \mathbb{Z}_{>0}$ form a PPT, that is $(x, y, z) = 1$ and $x^2 + y^2 = z^2$.

Suppose $2 \nmid xy$ then $z^2 \equiv x^2 + y^2 \equiv 2 \pmod 4$ which is impossible from the above. We conclude that $2 \mid xy$ and WLOG we suppose $2 \mid y$; furthermore, x and z are odd because we know that $(y, x) = (x, z) = 1$.

Note that $a^2 \equiv 1 \pmod 8$ for any odd integer a, because

$$1^2 \equiv 1, \quad 3^2 = 9 \equiv 1, \quad 5^2 = 25 \equiv 1, \quad 7^2 = 49 \equiv 1 \pmod 8.$$

Therefore, $y^2 = z^2 - x^2 \equiv 1 - 1 \equiv 0 \pmod 8$, hence $8 \mid y^2$.

We have $y^2 = y \cdot y = 2 \cdot 2 \cdot 2 \cdot k$, for some integer $k \neq 0$. Since 2 is prime, we must have $2 \mid y$, i.e $y = 2k_y$; thus $2k_y \cdot 2k_y = 2 \cdot 2 \cdot 2 \cdot k$ which implies $k_y^2 = 2 \cdot k$, hence $2 \mid k_y$. We conclude that $4 \mid y$.

Exercise 6. We want to show that the integers given by $x_1 = 3$, $y_1 = 4$, $z_1 = 5$ and

$$x_{n+1} = 3x_n + 2z_n + 1, \quad x_{n+1} = 3x_n + 2z_n + 2, \quad x_{n+1} = 4x_n + 3z_n + 2,$$

define a PT for all $n \geq 1$. We note that the values produced by these formulas are always positive. We will use induction on n to show they also satisfy the Pythagorean relation.

Base: $n = 1$**.** Clearly

$$x_1^2 + y_1^2 = 3^2 + 4^2 = 25 = 5^2 = z_1^2,$$

so that x_1, y_1, z_1 form a PT.

Induction hypothesis: $x_{n-1}^2 + y_{n-1}^2 = z_{n-1}^2$.

Inductive Step: $n > 1$**.** First we observe that

$$y_n = x_n + 1$$

and

$$\begin{aligned} z_n^2 &= (4x_{n-1} + 3z_{n-1} + 2)^2 \\ &= 16x_{n-1}^2 + 24x_{n-1}z_{n-1} + 16x_{n-1} + 12z_{n-1} + 9z_{n-1}^2 + 4. \end{aligned}$$

We now compute

$$\begin{aligned} x_n^2 + y_n^2 &= x_n^2 + (x_n + 1)^2 \\ &= 2x_n^2 + 2x_n + 1 \\ &= 2(3x_{n-1} + 2z_{n-1} + 1)^2 + 2(3x_{n-1} + 2z_{n-1} + 1) + 1 \\ &= 18x_{n-1}^2 + 24x_{n-1}z_{n-1} + 18x_{n-1} + 12z_{n-1} + 8z_{n-1}^2 + 5 \\ &= (2x_{n-1}^2 + 2x_{n-1} + 1) + (16x_{n-1}^2 + 24x_{n-1}z_{n-1} + 16x_{n-1} + 12z_{n-1} + 8z_{n-1}^2 + 4) \\ &= x_{n-1}^2 + y_{n-1}^2 + (16x_{n-1}^2 + 24x_{n-1}z_{n-1} + 16x_{n-1} + 12z_{n-1} + 8z_{n-1}^2 + 4) \\ &= z_{n-1}^2 + (16x_{n-1}^2 + 24x_{n-1}z_{n-1} + 16x_{n-1} + 12z_{n-1} + 8z_{n-1}^2 + 4) \\ &= 16x_{n-1}^2 + 24x_{n-1}z_{n-1} + 16x_{n-1} + 12z_{n-1} + 9z_{n-1}^2 + 4 \\ &= z_n^2, \end{aligned}$$

where in the third to last equality we have used the induction hypothesis and on the last equality we used the expression for z_n^2 above. We conclude that

$$x_n^2 + y_n^2 = z_n^2,$$

that is x_n, y_n, z_n is a Pythagorean triple, as desired.

Exercise 13. Suppose that x, y, z is a PT with $z = y + 2$. Then

$$x^2 + y^2 = z^2 = (y + 2)^2 = y^2 + 4y + 4,$$

so that

$$x^2 = 4(y + 1)$$

and, in particular, $2 \mid x^2$. Thus $2 \mid x$ and $x = 2k$ for some $k \in \mathbb{Z}_{>0}$. Substituting this back into the formula $x^2 = 4(y + 1)$ yields

$$x^2 = (2k)^2 = 4k^2 = 4(y + 1),$$

so that $y = k^2 - 1$. Lastly, since $z = y + 2$, we have $z = k^2 + 1$ and therefore the triple (x, y, z) is of the form

$$(x, y, z) = (2k, k^2 - 1, k^2 + 1).$$

Finally, we let $k \in \mathbb{Z}_{>0}$ and observe that

$$(2k)^2 + (k^2 - 1)^2 = 4k^2 + k^4 - 2k^2 + 1 = k^4 + 2k^2 + 1 = (k^2 + 1)^2,$$

that is, for all $k > 0$ the expression above produces PT such that $z = y + 2$.

Section 13.2

Exercise 3. Recall Fermat's Little Theorem: if $a \in \mathbb{Z}$ satisfies $(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

(a) Clearly, if $p \mid x$, $p \mid y$ or $p \mid z$ then $p \mid xyz$. We now prove the contrapositive statement. Suppose $p \nmid xyz$, then $p \nmid x$, $p \nmid y$, and $p \nmid z$, hence by FLT

$$x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \equiv 1 \pmod{p}.$$

Therefore,

$$x^{p-1} + y^{p-1} \equiv 1 + 1 = 2 \not\equiv 1 \equiv z^{p-1} \pmod{p},$$

as desired.

(b) It follows from FLT that for any integer a we have $a^p \equiv a \pmod{p}$. Then,

$$x^p + y^p = z^p \implies x + y \equiv z \pmod{p} \Leftrightarrow p \mid (x + y - z),$$

as desired.

Exercise 5. We assume that $x^4 - y^4 = z^2$ has no solutions in non-zero integers.

Let x, y be the length of the legs and z the length of the hypotenuse of a right triangle with integer sides. WLOG we can assume that x, y, z form a PPT with even y. That is

$$x^2 + y^2 = z^2, \qquad (x, y, z) = 1, \qquad y = 2k, \quad k \in \mathbb{Z}.$$

From the classification of PPT (Theorem 13.1 in Rosen) we know there are coprime integers m, n such that

$$m > n > 0, \qquad x = m^2 - n^2, \qquad y = 2mn, \qquad z = m^2 + n^2.$$

Suppose now the area of the triangle is a square, that is

$$\text{Area} = \frac{1}{2}xy = (m^2 - n^2)mn = r^2, \quad r \in \mathbb{Z}_{>0}.$$

Since m, n and $m^2 - n^2$ are positive and pairwise coprime it follows that they are squares (by Proposition left as homework in class). More precisely, there are positive integers a, b and c such that

$$m = a^2, \qquad n = b^2 \qquad m^2 - n^2 = c^2.$$

It now follows that $a^4 - b^4 = c^2$ which contradicts the first sentence.