MATH 135 — Fall 2021
Practice Problems (Solutions)– Chapters 6, 7, and 8

Mark Girard

December 3, 2021

Topics: divisibility, gcd, linear Diophantine equation, Euclidean Algorithm, prime factorizations, and modular arithmetic. (Problems are in no particular order.)

1. Determine $d = \gcd(339, -2145)$ and find integers s and t such that $399s - 2145t = d$.

Solution. We can use the Extended Euclidean Algorithm to compute $\gcd(2145, 339)$, which produces the following table:

	x	y	r
R_1	1	0	2145
R_2	0	1	339
$R_1 - 6R_2 = R_3$	1	-6	111
$R_2 - 3R_3 = R_4$	-3	19	6
$R_3 - 18R_4 = R_5$	55	-348	3
$R_4 - 2R_5 = R_6$	-113	715	0

From the table, we see that $2145 \cdot (55) + 339 \cdot (-358) = 3$. It follows that

$$339 \cdot (-348) - 2145 \cdot (-55) = 3,$$

where $3 = \gcd(2145, 339) = \gcd(339, -2145)$.

2. Prove the following statement:

For all $a, b, c \in \mathbb{Z}$, if $\gcd(a, b) = 1$ and $a \mid c$ and $b \mid c$, then $ab \mid c$.

Solution.

Proof. Let $a, b, c \in \mathbb{Z}$. Assume that $\gcd(a, b) = 1$ and $a \mid c$ and $b \mid c$. By CCT, there exists integers $x, y \in \mathbb{Z}$ such that $ax + by = 1$. By the definition of divisibility, there exists $k, \ell \in \mathbb{Z}$ such that $ak = c$ and $b\ell = c$. Note that $b\ell = ak$ which implies that $b \mid ak$. Because $\gcd(a, b) = 1$, it follows from CAD that $b \mid k$. Hence there exists an integer $m \in \mathbb{Z}$ such that $bm = k$. Now,

$$c = ak = abm$$

and thus $ab \mid c$ as desired. □

3. Prove or disprove the following statement

For all integers $x, y, z \in \mathbb{Z}$, if $x \mid yz$ then $x \mid y$ or $x \mid z$.

Solution. This statement is false. It's negation is the following statement:

There exist integers $x, y, z \in \mathbb{Z}$ such that $x \mid yz$ but $x \nmid y$ and $x \nmid z$.

Proof (of the negation). Let $x = 6$, $y = 2$ and $z = 3$. Then $x \mid yz$ because $6 \mid 6$, but $6 \nmid 2$ and $6 \nmid 3$. □

4. Prove, for all positive integers d, m, and n, that if $d = \gcd(m, n)$ then for all positive integers k it holds that $\gcd(m, nk) = \gcd(m, dk)$.

Solution.

Proof. Let $d = \gcd(m, n)$. By Bezout's Lemma, there exist integers $s, t \in \mathbb{Z}$ such that

$$ms + nt = d.$$

Let $k \in \mathbb{N}$ be an arbitrary positive integer and define $e = \gcd(m, nk)$. By Bezout's Lemma, there exist integers $x, y \in \mathbb{Z}$ such that

$$mx + nky = e.$$

Moreover, because $e \mid m$ and $e \mid nk$, there exist integers $a, b \in \mathbb{Z}$ such that $m = ae$ and $nk = be$. Now

$$\begin{aligned} dk &= (ms + nt)k && \text{[Because } d = ms + nt\text{]} \\ &= mks + nkt \\ &= aeks + bet && \text{[Because } m = ae \text{ and } nk = be\text{]} \\ &= e(aks + bt) \end{aligned}$$

and thus $e \mid dk$. Hence e is a common divisor of m and dk. Moreover, because $d \mid n$, there is an integer c such that $dc = n$. Now

$$\begin{aligned} e &= mx + nky \\ &= mx + dcky && \text{[Because } n = dc\text{]} \\ &= mx + (dk)(ny). \end{aligned}$$

Thus, by the GCD Charaterization Theorem, it follows that $e = \gcd(m, dk)$. This completes the proof. □

5. Let a and b be integers, let $d = \gcd(a, b)$, and consider the set $S = \{ax + by : x, y \in \mathbb{Z}\}$. Prove that
$$S = \{kd : k \in \mathbb{Z}\}$$

Solution.

Proof.

- We first prove that $S \subseteq \{kd : k \in \mathbb{Z}\}$. Let $n \in S$ be an arbitrary element of S. Then there are integers $x, y \in \mathbb{Z}$ such that $ax + by = n$. Because $d \mid a$ and $d \mid b$, it follows that $d \mid n$ by DIC. Thus, there exists an integer $k \in \mathbb{Z}$ such that $n = kd$, which means that $n \in \{kd : k \in \mathbb{Z}\}$.

- We next prove that $\{kd : k \in \mathbb{Z}\} \subseteq S$. Let $n \in \{kd : k \in \mathbb{Z}\}$ so that there is an integer $k \in \mathbb{Z}$ satisfying $n = kd$. By B'ezout's Lemma, there exists a choice of integers $s, t \in \mathbb{Z}$ such that $as + bt = d$. Choose $x = ks$ and $y = kt$, which are integers. Then
$$ax + by = kas + kbt = k(as + bt) = kd = n$$
and thus $n \in S$.

Thus we have proved that $S \subseteq \{kd : k \in \mathbb{Z}\}$ and $\{kd : k \in \mathbb{Z}\} \subseteq S$, so it follows that $S = \{kd : k \in \mathbb{Z}\}$. □

6. Prove that, for all prime numbers p and q, $\{px + qy : x, y \in \mathbb{Z}\} = \mathbb{Z}$ if and only if $p \neq q$.

Solution.

Proof. Let p and q be prime numbers, let $d = \gcd(p, q)$, and define
$$S = \{px + qy : x, y \in \mathbb{Z}\}.$$
From Problem 5, it holds that $S = \{kd : k \in \mathbb{Z}\}$.

- [To prove $p \neq q \implies S = \mathbb{Z}$.] Assume that $p \neq q$. The positive divisors of p are 1 and p, while the positive divisors of q are 1 and q. Because $p \neq q$, it follows that $d = \gcd(p, q) = 1$. Now, $S = \{k : k \in \mathbb{Z}\} = \mathbb{Z}$, as desired.

- [To prove $p = q \implies S \neq \mathbb{Z}$.] Assume that $p = q$. Then $d = \gcd(p, q) = p$ and thus $S = \{kp : k \in \mathbb{Z}\}$. Note that $1 \notin S$. Indeed, if it were the case that $1 \in S$, then there would be an integer $k \in \mathbb{Z}$ such that $1 = kp$, which is a contradiction, as p does not divide 1. Thus $\mathbb{Z} \nsubseteq S$, which implies that $S \neq \mathbb{Z}$.

This completes the proof. □

7. Let $a = 3^2 5^3 7^4 13^1$, $b = 5^1 7^2 13^2 23^9$, and $c = 3 \cdot 5 \cdot 7 \cdot 13 \cdot 23$.

   (a) Determine $\gcd(a, b)$.

Solution. The greatest common divisor of these numbers is given by

$$\begin{aligned}\gcd(a,b) &= 3^{\min\{2,0\}} \cdot 5^{\min\{3,1\}} \cdot 7^{\min\{4,2\}} \cdot 13^{\min\{1,2\}} \cdot 23^{\min\{0,9\}} \\ &= 3^0 \cdot 5^1 \cdot 7^2 \cdot 13^1 \cdot 23^0 \\ &= 5 \cdot 7^2 \cdot 13\end{aligned}$$

(b) What is the smallest integer t such that $a \mid c^t$ and $b \mid c^t$?

Solution. The answer is 9. Indeed, when $t = 9$, note that

$$c^t = c^9 = 3^9 \cdot 5^9 \cdot 7^9 \cdot 13^9 \cdot 23^9,$$

which is divisible by both a and b. For every integer $t < 9$, one has that $23^9 \nmid c^t$ because $9 \not\leq t$ and thus $b \nmid c^t$.

8. Suppose $a \in \mathbb{Z}$ and consider the statement P: "if $24 \mid a^2$ then $36 \mid a^3$".

(a) Prove P.

(b) Prove or disprove the converse of P.

Solution.

(a)
- [*Solution 1.*] Suppose that $24 \mid a^2$. Note that $12 \mid 24$ and that $3 \mid 24$, and thus $12 \mid a^2$ and $3 \mid a^2$ by Transitivity of Divisibility. Because 3 is prime, it follows from Euclid's Lemma that $3 \mid a$. Now $12 \mid a^2$ and $3 \mid a$, so it follows that $(12 \cdot 3) \mid a^3$. Hence $36 \mid a^3$ as desired.
- [*Solution 2*]. Note that the prime factorisation of 24 is $2^3 \cdot 3^1$. Hence the prime factorization of a must include at least 2 and 3 in its list of prime factors,

$$a = 2^k \cdot 3^\ell \cdot p_3^{\alpha_3} \cdots p_n^{\alpha_n},$$

where $k, \ell \geq 1$. Now,

$$\begin{aligned}a^3 &= 2^{3k} \cdot 3^{3\ell} \cdot p_3^{3\alpha_3} \cdots p_n^{3\alpha_n} \\ &= (2^3 \cdot 3^3) \cdot 2^{3(k-1)} \cdot 3^{3(\ell-1)} \cdot p_3^{3\alpha_3} \cdots p_n^{3\alpha_n} \\ &= 36 \cdot 6 \cdot 2^{3(k-1)} \cdot 3^{3(\ell-1)} \cdot p_3^{3\alpha_3} \cdots p_n^{3\alpha_n}\end{aligned}$$

and thus $36 \mid a^3$.

(b) The converse of P is"If $36 \mid a^3$ then $24 \mid a^2$." The converse of P is false. Indeed, consider $a = 6$. Then $a^3 = 6^2 \cdot 6 = 36 \cdot 6$ so $36 \mid a^3$. But $a^2 = 36$ and $24 \nmid 36$ so $24 \nmid a^2$.

9. Suppose a and b are positive integers and let c be an integer such that $\gcd(a,b) \mid c$. Prove

that there exists a unique integer solution (x', y') to the linear Diophantine Equation

$$ax + by = c$$

such that $0 \leq x' < \frac{b}{\gcd(a,b)}$.

Solution.

Proof. By the Linear Diophantine Equaion Theorem, there exists an integer solution (x_0, y_0) because $\gcd(a, b) \mid c$. By the Division Algorithm, because $\frac{b}{\gcd(a,b)} > 0$, there exists a unique choice of integers $q, r \in \mathbb{Z}$ such that

$$x_0 = q\frac{b}{\gcd(a,b)} + r \qquad \text{and} \qquad 0 \leq r < \frac{b}{\gcd(a,b)}.$$

Now define $x' = x_0 - q\frac{b}{\gcd(a,b)}$ and $y' = y_0 + q\frac{a}{\gcd(a,b)}$. By the Linear Diophantine Equation Theorem, it holds that (x', y') is also a solution to this equation. Note that

$$x' = r$$

and thus $0 \leq x' < \frac{b}{\gcd(a,b)}$. It remians to prove that this solution is unique.

To prove that (x', y') is unique, let (x'', y'') be another solution to the Diophantine equation such that $0 \leq x'' < \frac{b}{\gcd(a,b)}$. By the Linear Diophantine Equation Theorem, there exists an integer $n \in \mathbb{Z}$ such that

$$x'' = x_0 - n\frac{b}{\gcd(a,b)} \qquad y'' = y_0 + n\frac{a}{\gcd(a,b)}.$$

In particular, note that

$$x_0 = \frac{b}{\gcd(a,b)} + x''.$$

By the Division Algorithm, it must be the case that $m = q$ and $x'' = x'$. This completes the proof. □

10. Suppose that Canada Post issued 49¢ and 53¢ stamps. How many different ways could you purchase exactly \$100 worth of these kinds of stamps?

Solution. We need to find all solutions to the linear Diophantine equation

$$49x + 53y = 10000. \qquad (*)$$

We can use the Extended Euclidean Algorithm to compute $\gcd(49, 53)$, which produces the following table:

	x	y	r
R_1	1	0	53
R_2	0	1	49
$R_1 - 1R_2 = R_3$	1	-1	4
$R_2 - 12R_3 = R_4$	-12	13	1

From the table above, we see that $\gcd(53, 49) = 1$ and moreover that

$$53(-12) + 49(13) = 1.$$

Multiplying this by 10000, we see that one solution to the equation ($*$) is

$$x_0 = 130000 \qquad \text{and} \qquad y_0 = -120000$$

and sll other solutions are of the form

$$x = x_0 - 53n \qquad \text{and} \qquad y = y_0 + 49n$$

for some $n \in \mathbb{Z}$. The set of valid solutions having $x \geq 0$ and $y \geq 0$ is described as

$$S = \{(x_0 - 53n, y_0 + 49n) \,:\, n \in \mathbb{Z},\, x_0 - 53n \geq 0 \text{ and } y_0 + 49n \geq 0\}.$$

(These are the solutions where the numbers of stamps of both types are both positive.) Note that

$$120000 = 49 \cdot 2449 - 1$$

and thus

$$\begin{aligned} y_0 + 49 \cdot 2449 &= -120000 + 49 \cdot 2449 \\ &= 1 \end{aligned}$$

and also

$$\begin{aligned} x_0 - 53 \cdot 2449 &= 130000 - 129797 \\ &= 203. \end{aligned}$$

Hence, one solution (x_1, y_1) having $x_1 \geq 0$ and $y_1 \geq 0$ is

$$x_1 = 203 \qquad \text{and} \qquad y_0 = 1.$$

All valid solutions are of the form $(203 - 53n, 1 + 49n)$ for some integer n such that $203 - 53n \geq 0$ and $1 + 49n \geq 0$. The valid soltions are therefore

$$\begin{aligned} &(203, 1) \\ (203 - 53, 1 + 49) = &(150, 50) \\ (203 - 2 \cdot 53, 1 + 2 \cdot 49) = &(97, 99) \\ (203 - 3 \cdot 53, 1 + 3 \cdot 49) = &(44, 108). \end{aligned}$$

Hence there are only four ways to purchase exactly \$100 worth of 49¢ and 53¢ stamps. The solution set we are interested in is given by

$$\begin{aligned} S &= \{(x,y) \in \mathbb{Z}^2 \,:\, x \geq 0 \text{ and } y \geq 0 \text{ and } 49x + 53y = 10000\} \\ &= \{(203 - 53n, 1 + 49n) \,:\, n \in \mathbb{Z} \text{ and } 203 - 53n \geq 0 \text{ and } 1 + 49n \geq 0\} \\ &= \{(203,1), (150,50), (97,99), (44,108)\}, \end{aligned}$$

which contains only 4 elements.

11. Let n be a positive integer. Prove the following statements.

(a) If n is odd, then $n^2 \equiv 1 \pmod 8$.

Solution. Let n be an odd integer. Then either $n \equiv 1 \pmod 8$, $n \equiv 3 \pmod 8$, $n \equiv 5 \pmod 8$, or $n \equiv 7 \pmod 8$. Let's consider each case separately.

- If $n \equiv 1 \pmod 8$, then $n^2 \equiv 1^2 \equiv 1 \pmod 8$.
- If $n \equiv 3 \pmod 8$, then $n^2 \equiv 3^2 \equiv 9 \equiv 1 \pmod 8$.
- If $n \equiv 5 \pmod 8$, then $n^2 \equiv 5^2 \equiv 25 \equiv 8 \cdot 3 + 1 \equiv 1 \pmod 8$.
- If $n \equiv 7 \pmod 8$, then $n^2 \equiv 7^2 \equiv 49 \equiv 8 \cdot 6 + 1 \equiv 1 \pmod 8$.

In every case, it holds that $n^2 \equiv 1 \pmod 8$.

(b) If $n^2 \not\equiv 1 \pmod 3$, then $n \equiv 0 \pmod 3$.

Solution. We prove the converse, which states: "If $n \not\equiv 0 \pmod 3$, then $n^2 \equiv 1 \pmod 3$".

Proof. Suppose that $n \not\equiv 0 \pmod 3$. Then either $n \equiv 1 \pmod 3$ or $n \equiv 2 \pmod 3$. We consider both cases separately.

- If $n \equiv 1 \pmod 3$, then $n^2 \equiv 1^2 \equiv 1 \pmod 3$.
- If $n \equiv 2 \pmod 3$, then $n^2 \equiv 4 \equiv 3 + 1 \equiv 1 \pmod 3$.

In either case, it holds that $n^2 \equiv 1 \pmod 3$. □

12. Solve the equation $[9][x] = [5]$ in $\mathbb{Z}_{43}$.

Solution. We can use the Extended Euclidean Algorithm to compute $\gcd(43, 9)$, which produces the following table:

	x	y	r
R_1	1	0	43
R_2	0	1	9
$R_1 - 4R_2 = R_3$	1	-4	7
$R_2 - R_3 = R_4$	-1	5	2
$R_3 - 3R_4 = R_5$	4	-19	1

From the table, we see that $43 \cdot (4) - 9 \cdot (19) = 1$, and thus $9 \cdot 19 = 43 \cdot 4 - 1$, which implies that

$$9 \cdot 19 \equiv -1 \pmod{43}.$$

Multiplyting this congruence by -5 yields

$$9 \cdot (19 \cdot (-5)) \equiv 5 \pmod{43}.$$

Note that

$$19 \cdot (-5) \equiv -95 \equiv 3 \cdot 43 - 95 \equiv 129 - 95 \equiv 34 \pmod{43}.$$

Hence, we have that

$$[19][34] = [19][19 \cdot (-5)] = [5] \qquad \text{in } \mathbb{Z}_{43}.$$

Because $\gcd(9, 43) = 1$, there is only one solution, so the is the only solution is $[x] = [34]$.

13. (a) Find the units digit of 6012016^{20} (in base 10).

Solution. We need to find the remainder of 6012016^{20} when divided by 10. Note that $6012016 \equiv 6 \pmod{10}$ and thus

$$6012016^{20} \equiv 6^{20} \pmod{10}.$$

Next, we prove by induction that, for all $n \in \mathbb{N}$, it holds that $6^n \equiv 6 \pmod{10}$. Indeed, this is true for the Base Case, because $6^1 \equiv 6 \pmod{10}$. To prove the Induction Step, let $k \in \mathbb{N}$ ans suppose that $6^k \equiv 6 \pmod{10}$. Then

$$6^{k+1} \equiv 6^k \cdot 6 \equiv 6 \cdot 6 \equiv 36 \equiv 6 \pmod{10}.$$

By the Principle of Mathematical Induction, it holds that $6^n \equiv 6 \pmod{10}$ for all $n \in \mathbb{N}$. We may conclude that $6^{20} \equiv 6 \pmod{10}$ and thus the units digit of 6012016^{20} is 6.

(b) Find the last two digits of 7^{1942} in base 10.

Solution. To find the last two digits, we need to find the remainder of 7^{1942} when divided by 100. Now, $7^2 = 49$ and note that[a]

$$\begin{aligned} 49^2 = (50-1)^2 &= 50^2 - 2\cdot 50 + 1 \\ &= 100\cdot 25 - 100 + 1 \\ &= 100 \cdot 24 + 1 \end{aligned}$$

and thus $49^2 \equiv 1 \pmod{100}$. Hence,

$$7^4 \equiv (49)^2 \equiv 1 \equiv \quad \pmod{100}.$$

Next, note that

$$\begin{aligned} 1942 &= 194 \cdot 10 + 2 \\ &= (97\cdot 2)\cdot(2\cdot 5) + 2 \\ &= 4k + 2 \end{aligned}$$

where $k = 97 \cdot 5$. Hence,

$$7^{1942} \equiv 7^{4\cdot 97\cdot 5 + 2} \equiv (7^4)^{97\cdot 5} \cdot 7^2 \equiv 1 \cdot 49 \equiv 49 \pmod{100}.$$

Hence the last two digits of 7^{1942} are 49.

[a] Alternatively, one may mulitply out to find that $49^2 = 2401$.

14. Prove the following facts about the binomial coefficient.

(a) For all non-negative integers $n, k \in \mathbb{Z}$, it holds that $\binom{n}{k} \in \mathbb{Z}$.

Solution. We prove by induction. For each non-negative integer n, let $P(n)$ be the statement that "For all non-negative integers k, it holds that $\binom{n}{k} \in \mathbb{Z}$."

- Base case: By definition, one has $\binom{0}{0} = 1$ and $\binom{0}{k} = 0$ whenever $k > 0$. Thus $\binom{0}{k}$ is an integer for every non-negative integer k. Hence $P(0)$ is true.
- Induction Step: Let m be a non-negative integer and assume that $P(m)$ is true. That is, assume that $\binom{m}{\ell}$ is an integer for every non-negative integer ℓ. We prove that $\binom{m+1}{k}$ is an integer for every non-negative integer k. Let $k \in \mathbb{Z}$ be an arbitrary non-negative integer. There are two cases:
  - If $k < m+1$, then by Pascal's Identity, it holds that

$$\binom{m+1}{k} = \binom{m}{k} + \binom{m}{k+1},$$

which is an integer, because $\binom{m}{k}$ and $\binom{m}{k+1}$ are integers by the Induction Hypothesis.

– If $k = m+1$, then $\binom{m+1}{k} = \binom{m+1}{m+1} = 1$, which is an integer.

– If $k > m+1$, then $\binom{m+1}{k} = 0$ by definition, which is an integer.

In each case, we see that $\binom{m+1}{k}$ is an integer. Hence $P(m+1)$ is true.

By the principle of induction, it holds that $\binom{n}{k}$ is an integer for all non-negative integers $n, k \in \mathbb{Z}$.

(b) Let p be a prime number. It holds that

$$\binom{p}{k} \equiv 0 \pmod{p}$$

for all $k \in \{1, 2, \ldots, p-1\}$.

Solution.

Proof. Let $k \in \{1, 2, \ldots, p-1\}$. By definition, we have that

$$\binom{p}{k} = \frac{p!}{k!(p-k)!},$$

and thus

$$\begin{aligned} p \cdot (p-1)! = p! &= k!(p-k)!\binom{p}{k} \\ &= (1 \cdot 2 \cdot \cdots \cdot k)(1 \cdot 2 \cdot \cdots \cdot (p-k))\binom{p}{k}, \end{aligned}$$

and thus $p \mid \left(k!(p-k)!\binom{p}{k}\right)$. Note also that

$$\gcd(p,1) = \gcd(p,2) = \cdots = \gcd(p, p-1) = 1.$$

Because $1 \leq k \leq p-1$ and $1 \leq p-k \leq p-1$, it follows that

$$\gcd\big(p, k!(p-k)!\big) = 1.$$

Because $p \mid \left(k!(p-k)!\binom{p}{k}\right)$ and $\gcd\big(p, k!(p-k)!\big) = 1$, it follows from Euclid's Lemma that

$$p \mid \binom{p}{k}.$$

This implies that $\binom{p}{k} \equiv 0 \pmod{p}$. □

15. Prove the following statements.

(a) The sum of any three consecutive natural numbers is divisible by 3.

Solution. Symbolically, we can express this statement as:

$$\forall n \in \mathbb{Z},\ 3 \mid \big(n + (n+1) + (n+2)\big)$$

Proof. Let $n \in \mathbb{Z}$ be arbitrary. Now,

$$\begin{aligned} n + (n+1) + (n+2) &\equiv 3n + 3 && \pmod 3 \\ &\equiv 3(n+1) && \pmod 3 \\ &\equiv 0 && \pmod 3, \end{aligned}$$

and thus $3 \mid \big(n + (n+1) + (n+2)\big)$. □

(b) The sum of any four consecutive natural numbers is NOT divisible by 4.

Solution. Symbolically, we can express this statement as:

$$\forall n \in \mathbb{Z},\ 4 \nmid \big(n + (n+1) + (n+2) + (n+3)\big)$$

Proof. Let $n \in \mathbb{Z}$ be arbitrary. Now,

$$\begin{aligned} n + (n+1) + (n+2) + (n+3) &\equiv 4n + 1 + 2 + 3 && \pmod 4 \\ &\equiv 4n + 7 && \pmod 4 \\ &\equiv 7 && \pmod 4, \end{aligned}$$

but $4 \nmid 7$ and thus $4 \nmid \big(n + (n+1) + (n+2) + (n+3)\big)$. □

16. Let $x \in \mathbb{Z}$. Prove that $4x^2 + x + 3$ is not divisible by 5.

Solution. We only need to consider $x \in \{0, 1, 2, 3, 4\}$. Construct the following table:

x	0	1	2	3	4
x^2	0	1	4	9	16
$x^2 \pmod 5$	0	1	4	4	1
$4x^2 \pmod 5$	0	4	1	1	4
$4x^2 + x + 3 \pmod 5$	3	3	1	2	1

Note that $4x^2 + x + 3 \not\equiv 0 \pmod 5$ for each x, and thus $4x^2 + x + 3$ is never divisible by 5.

17. Let p be a prime number. Prove the following statement:

$$\text{There exists an integer } n \in \mathbb{Z} \text{ such that } n^3 = p + 8 \qquad \Longleftrightarrow \qquad p = 19.$$

Solution. If $p = 19$, then $p + 8 = 19 + 8 = 27$ and we may choose $n = 3$ such that $n^3 = 27$. Conversely, suppose that there exists an integer $n \in \mathbb{Z}$ such that $n^3 = p + 8$. It follows that $n^3 - 8 = p$ and thus

$$(n-2)(n^2+2n+4) = p.$$

We first prove that $n^2 + 2n + 4 > 1$.

- If $n \geq 0$, then $n^2 + 2n + 4 \geq 4$.
- If $n = -1$, then $n^2 + 2n + 4 = 3$.
- If $n < -1$, then $n \leq -2$ which implies $n^2 \geq -2n$ and thus $n^2 + 2n \geq 0$. Hence $n^2 + 2n + 4 \geq 4$.

In each case, we have $n^2 + 2n + 4 > 1$. Because p is prime, its only poisitive divisors are 1 and p, so it must therefore be the case that

$$n - 2 = 1 \qquad \text{and} \qquad n^2 + 2n + 4 = p.$$

That is, $n = 3$ and $p = n^2 + 2n + 4 = 9 + 6 + 4 = 19$.

18. Let $a, b \in \mathbb{Z}$ and let p be a prime number. Prove that $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Solution. There are two ways to prove this.

- *Proof 1.* Using the Binomial Theorem, we have

$$\begin{aligned}
(a+b)^p &= \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k \\
&= \binom{p}{0} a^p b^0 + \binom{p}{1} a^{p-1} b^1 + \cdots + \binom{p}{p-1} a^1 b^{p-1} + \binom{p}{p} a^0 b^p \\
&= a^p + \binom{p}{1} a^{p-1} b^1 + \cdots + \binom{p}{p-1} a^1 b^{p-1} + b^p.
\end{aligned}$$

However, from problem 14b we see that

$$\binom{p}{k} \equiv 0 \pmod{p}$$

for every $k \in \{1, 2, \ldots, p-1\}$, and thus

$$\begin{aligned}
(a+b)^p &\equiv a^p + \binom{p}{1} a^{p-1} b^1 + \cdots + \binom{p}{p-1} a^1 b^{p-1} + b^p && \pmod{p} \\
&\equiv a^p + 0 + \cdots + 0 + b^p && \pmod{p} \\
&\equiv a^p + b^p && \pmod{p}.
\end{aligned}$$

- *Proof 2.* From the Corollary to Fermat's Little Theorem, it holds that

  $$a^p \equiv a \pmod{p}, \quad b^p \equiv b \pmod{p}, \quad \text{and } (a+b)^p \equiv a+b \pmod{p}.$$

  Thus
  $$(a+b)^p \equiv a+b \equiv a^p + b^p \pmod{p}.$$