Solutions to Introduction to Analytic Number Theory

Susam Pal

Contents

Chapter 1

The Fundamental Theorem of Arithmetic

In these exercises lower case latin letters a, b, c, $\ldots$, x, y, z represent integers. Prove each of the statements in Exercises 1.1 through 1.6.

Exercise 1.1. If $(a, b) = 1$ and if $c \mid a$ and $d \mid b$, then $(c, d) = 1$.

Example. Let $a = 6$ and $b = 35$, so we have $(a, b) = (6, 35) = 1$. Let $c = 2$ and $d = 5$. We see that $2 \mid 6$ and $5 \mid 35$ and indeed $(2, 5) = 1$.

Another example. Let $a = 0$ and $b = 1$. Let $c = 2$ and $d = 1$. We see that $c \mid a$ and $d \mid b$ and indeed $(c, d) = 1$.

Proof. Let $(c, d) = g$. Since $g \mid c$ and $c \mid a$, by the transitive property of divisibility in Theorem 1.1 (b), $g \mid a$. Similarly, $g \mid b$. By the definition of gcd in section 1.3, we know that every common divisor of a and b divides (a, b), therefore $g \mid 1$. Since the only nonnegative integer that divides 1 is 1 itself, $g = 1$. $\square$

Another proof. Since $(a, b) = 1$, by Theorem 1.2 and the definition of gcd in section 1.3, we know that there are integers x and y such that $ax + by = 1$. Since $c \mid a$ and $d \mid b$, we have $a = cm$ and $b = dn$. Therefore $c(mx) + d(ny) = (cm)x + (dn)y = ax + by = 1$. This implies $(c, d) = 1$. □

Exercise 1.2. If $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.

Example. Let $a = 35$, $b = 6$, and $c = 14$, so we have $(a, b) = (35, 6) = 1$ and $(35, 14) = 1$. Indeed $(a, bc) = (35, 84) = 1$.

Proof. We assume $(a, bc) > 1$ and obtain a contradiction. Since $(a, bc) > 1$, from the fundamental theorem of arithmetic show in Theorem 1.10, we know that there is a prime p such that $p \mid (a, bc)$. By the definition of gcd in section 1.3, we know that $p \mid a$ and $p \mid bc$. If $p \mid bc$, from Thereom 1.9 we know that $p \mid b$ or $p \mid c$. If $p \mid a$ and $p \mid b$, from the definition of gcd we know that $p \mid (a, b)$. But $(a, b) = 1$. Since the only nonnegative integer that divides 1 is 1 itself, we have obtained a contradiction. If $p \mid a$ and $p \mid c$, we obtain a contradiction similarly. Thus $(a, bc) = 1$. □

Another proof. This proof avoids the use of the fundamental theorem of arithmetic. Let $d = (a, bc)$. We will first show that $(d, b) = 1$ and then conclude later that $d = 1$. Let $(d, b) = e$. Since $e \mid d$ and $d \mid a$, by the transitive property of divisibility in Theorem 1.1 (b), we get $e \mid a$. Since $e \mid a$ and $e \mid b$, by the definition of gcd and Theorem 1.3 (c), we get $e \mid (a, b) = 1$. Since $e \geq 0$ by the definition of gcd and since the only nonnegative integer that divides 1 is 1 itself, $e = 1$, i.e., $(d, b) = 1$. Since $d \mid bc$ and $(d, b) = 1$, by Thereom 1.5, we get $d \mid c$. Since $d \mid a$ and $d \mid c$, from the definition of gcd, we get $d \mid (a, c) = 1$. Thus $d = 1$. □

Yet another proof. This is a simple proof that depends only on the propeties of gcd shown in section 1.3. Since $(a, b) = 1$ and $(a, c) = 1$, there exist integers x_1, y_1, x_2, and y_2 such that

$$
\begin{aligned}
ax_1 + by_1 &= 1, \\
ax_2 + cy_2 &= 1.
\end{aligned}
$$

Therefore $(ax_1 + by_1)(ax_2 + cy_2) = 1$
$\iff a(ax_1x_2 + cx_1y_2 + by_1x_2) + bc(y_1y_2) = 1$. Therefore (a, bc) = 1. $\square$

Exercise 1.3. If $(a, b) = 1$, then $(a^n, b^k) = 1$ for all $n \leq 1$, $k \leq 1$.

Proof. We assume $(a^n, b^n) > 1$ and obtain a contradiction. Since $(a^n, b^n) > 1$, from the fundamental theorem of arithmetic shown in Theorem 1.10, we know that there is a prime p such that $p \mid (a^n, b^n)$. Since $p \mid a^n$, from Theorem 1.9 we know that $p \mid a$. Similarly, we know that $p \mid b$. Since $p \mid a$ and $p \mid b$, from the definition of gcd in section 1.3, we get $p \mid (a, b) = 1$. This is a contradiction because the only nonnegative integer that divides 1 is 1 itself. $\square$

Exercise 1.4. If $(a, b) = 1$, then $(a + b, a - b)$ is either 1 or 2.

Proof. Let $d = (a + b, a - b)$. If $a + b$ and $a - b$ are relatively prime, then $d = 1$. If they are not relatively prime, then $d > 1$. Then by the fundamental theorem of arithmetic shown in Theorem 1.10, there is a prime p such that $p \mid d$. From the definition of gcd in section 1.3, we get $p \mid (a + b)$ and $p \mid (a - b)$. From the linearity property of divisibility in Theorem 1.1 (c), we get $p \mid 2a$ and $p \mid 2b$. Now there are two cases to consider: $p \mid 2$ and $p \nmid 2$. If $p \mid 2$, $p = 2$ because the only prime that divides 2 is 2 itself. If $p \nmid 2$, by Theorem 1.8, we have $(p, 2) = 1$. If $p \mid 2a$ and $(p, 2) = 1$, then by Euclid's lemma shown in Theorem 1.5, we have $p \mid a$. We can similarly show that if $p \nmid 2$, then $p \mid b$. Thus by the definition of gcd, we get $p \mid (a, b) = 1$. Since the only positive integer that divides 1 is 1 itself, we have obtained a contradiction. Therefore, if $d > 1$, the only prime p such that $p \mid d$ is $p = 2$. Thus $d = 2$. We have shown that $d = 1$ or $d = 2$. $\square$

Another proof. This is a simpler proof that depends only on the properties of gcd. Since $(a, b) = 1$, from the definition of gcd in section 1.3, we know that there are integers x and y such that $ax + by = 1$. Therefore,

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

Thus from the linearity property in Theorem 1.1 (c), we know that $(a+b, a-b) \mid 2$. Now from the comparison property in Theorem 1.1 (i), we know that $(a+b, a-b) \leq 2$. □

Exercise 1.5. If $(a, b) = 1$, then $(a+b, a^2 - ab + b^2)$ is either 1 or 3.

Proof. Let $d = (a+b, a^2 - ab + b^2)$. If $(a+b)$ and $a^2 - ab + b^2$ are relatively prime, then $d = 1$. If they are not relatively prime, then $d > 1$. Then by the fundamental theorem of arithmetic in Theorem 1.10, there is a prime p such that $p \mid d$. From the definition of gcd in section 1.3, we get $p \mid (a+b)$ and $p \mid (a^2 - ab + b^2)$. From the linearity property of divisibility in Theorem 1.1 (c), we get $p \mid (a+b)^2 - (a^2 - ab + b^2) = 3ab$. Thus from Theorem 1.9, $p \mid 3$ or $p \mid a$ or $p \mid b$. If $p \mid a$, since $p \mid (a+b)$, using the linearity property of divisibility again, we see that $p \mid b$. But then by properties of gcd, $p \mid (a, b) = 1$. This is a contradiction, since the only positive integer that divides 1 is 1 itself. Therefore we conclude that $p \nmid a$. We can show similarly that $p \nmid b$. Thus we are left with only $p \mid 3$. Using the contrapositive of Theorem 1.9, we conclude that $p \nmid ab$. Thus using Theorem 1.8, we conclude that $(p, ab) = 1$. Since $p \mid 3ab$, using Euclid's Lemma in Theorem 1.5, we get $p \mid 3$. Thus $p = 3$. Therefore if $d > 1$, the only prime p such that $p \mid d$ is $p = 3$. We have shownt that $d = 1$ or $d = 3$. □

Exercise 1.6. If $(a, b) = 1$ and $d \mid (a+b)$, then $(a, d) = (b, d) = 1$.

Example. Let $a = 5$ and $b = 7$. Thus $a + b = 12$. We see that $2 \mid 12$ and indeed $(2, 5) = (2, 7) = 1$. We can pick any other divisor of d of 12 and indeed $(d, 5) = (d, 7) = 1$ holds.

Proof. Let $g = (a, d)$. By the definition of gcd in section 1.3, $g \mid a$ and $g \mid d$. Since $g \mid d$ and $d \mid (a + b)$, using the transitive property of divisiblity in Theorem 1.1 (b), we get $g \mid (a + b)$. Since $g \mid a$ and $g \mid (a+b)$, using the linearity property of divisibility in Theorem 1.1 (c), we get $g \mid b$. Since $g \mid a$ and $g \mid b$, using the property of gcd, we get $g \mid (a, b) = 1$. But the only nonnegative integer that divides 1 is 1 itself, therefore, $g = 1$. Therefore, $(a, d) = 1$. We can similarly show that $(b, d) = 1$. □

Exercise 1.7. A rational number a/b with $(a, b) = 1$ is called a *reduced fraction*. If the sum of two reduced fractions in an integer, say $(a/b) + (c/d) = n$, prove that $|-b| = |d|$.

Proof. Since $(a/b) + (c/d) = n$, we get $ad + bc = nbd$. Thus $ad = b(nd - c)$. This shows that $b \mid ad$. Since $b \mid ad$ and $(a, b) = 1$, from Euclid's lemma in Theorem 1.5 we get, $b \mid d$. We can similarly show that $d \mid bc$ and thus $d \mid b$. Since $b \mid d$ and $d \mid b$, from Theorem 1.1 (i), we get $|d| = |b|$. □

Exercise 1.8. An integer is called *squarefree* if it is not divisible by the square of any prime. Prove that for every $n \geq 1$ there exist uniquely determined $a > 0$ and $b > 0$ such that $n = a^2 b$, where b is squarefree.

Proof. TODO □

Chapter 5

Congruences

Exercise 5.1. Let S be a set of n integers (not necessarily distinct). Prove that some nonempty subset of S has a sum which is divisible by n.

Proof. Let $S = \{s_1, s_2, \ldots, s_n\}$. Let us define r_k such that

$$s_1 + s_2 + \cdots + s_k \equiv r_k \pmod{n}$$

where $0 \leq r_k < n$. Theorem 1.14 guarantees that such r_k exists for $k = 1, 2, \ldots, n$. Now consider the set

$$R = \{r_1, r_2, \ldots, r_n\}.$$

Either there exists r_m in R such that $r_m \equiv 0 \pmod{n}$ or no such r_m exists. If such an r_m exists, then $n \mid r_m$. If no such r_m exists then $1 \leq r_k < n$ for each r_k in R. Therefore each of the n elements in R can have one of $n-1$ values. By pigeonhole principle, there are at least two elements in R must have the same value. Let $r_i = r_j$ where $j > i$. Then $r_j - r_i = s_{i+1} + \cdots + s_j \equiv 0 \pmod{n}$. $\square$

Exercise 5.2. Prove that $5n^3 + 7n^5 \equiv 0 \pmod{12}$ for all integers n.

Proof. Let $f(n) = 5n^3 + 7n^5$. If $f(k) \equiv 0 \pmod{12}$ where k is an integer such that $0 \le k < 12$, then by Theorem 5.2 (b), $f(n) \equiv 0 \pmod{12}$ for all $n \equiv k \pmod{12}$. We can verify that $f(k) \equiv 0 \pmod{12}$ for $k = 0, 1, \ldots, 11$. Thus $f(n) \equiv 0 \pmod{12}$ for all $n \equiv k \pmod{12}$ for all $k = 0, 1, \ldots, 11$. By theorem Theorem 5.10 (c), $f(n) \equiv 0 \pmod{12}$ for all integers n. □

Another proof. Since $7 \equiv -5 \pmod{12}$, using 5.2 (a) we get

$$5n^3 + 7n^5 \equiv 5n^3 - 5n^5 \pmod{12}.$$

Now we want to solve

$$5n^3 - 5n^5 \equiv 0 \pmod{12}.$$

The above congruence can be rewritten as

$$5n^3(1+n)(1-n) \equiv 0 \pmod{12}.$$

We can verify that this congruence holds good for $n \equiv k \pmod 3$ for $k = 0, 1, 2$ and $n \equiv k \pmod 4$ for $k = 0, 1, 2, 3$. Thus the congruence holds good for $n \equiv k \pmod{12}$ for $k = 0, 1, 2, \ldots, 11$. □

Exercise 5.3 (a). Find all positive integers n for which $n^{13} \equiv n \pmod{1365}$.

Solution. Since $1365 = 3 \cdot 5 \cdot 7 \cdot 13$, we want to find all positive integers n such that $n^{13} \equiv n \pmod{3 \cdot 5 \cdot 7 \cdot 13}$. Using the Little Fermat Theorem from Theorem 5.19, we find that:

- For all integers n, $n^{13} = \left(n^3\right)^3 \cdot n^3 \cdot n \equiv n \cdot n \cdot n \equiv n^3 \equiv n \pmod 3$.
- For all integers n, $n^{13} = \left(n^5\right)^2 \cdot n^3 \equiv n^2 \cdot n^3 \equiv n^5 \equiv n \pmod 5$.
- For all integers n, $n^{13} = n^7 \cdot n^6 \equiv n \cdot n^6 \equiv n^7 \equiv n \pmod 7$.
- For all integers n, $n^{13} \equiv n \pmod{13}$.

Since 3, 5, 7, and 13 are relatively prime in pairs, we conclude that $n^{13} \equiv n \pmod{1365}$ for all integers n.

Exercise 5.3 (b). Find all positive integers n for which $n^{17} \equiv n \pmod{4080}$.

Solution. Since $4080 = 16 \cdot 3 \cdot 5 \cdot 17$, we want to find all positive integers n such that $n^{17} \equiv n \pmod{16 \cdot 3 \cdot 5 \cdot 17}$. Using the Little Fermat Theorem from Theorem 5.19, we get:

- For all integers n, $n^{17} = \left(n^3\right)^3 \cdot \left(n^3\right)^2 \cdot n^2 \equiv n \cdot n^2 \cdot n^2 \equiv n^3 \cdot n^2 \equiv n \cdot n^2 \equiv n^3 \equiv n \pmod 3$.
- For all integers n, $n^{17} = \left(n^5\right)^3 \cdot n^2 \equiv n^3 \cdot n^2 \equiv n^5 \equiv n \pmod 5$.
- For all integers n, $n^{17} \equiv n \pmod{17}$.

We can verify that $n^{17} \equiv n \pmod{16}$ if and only if $n \equiv k \pmod{16}$ where $k \in \{0, 1, 3, 5, 7, 9, 11, 13, 15\}$. Since 16, 3, 5, and 17 are relatively prime in pairs, we conclude that $n^{17} \equiv n \pmod{13}$ for all integers $n \equiv k \pmod{16}$ where $k \in \{0, 1, 3, 5, 7, 9, 11, 13, 15\}$.

Exercise 5.4 (a). Prove that $\varphi(n) \equiv 2 \pmod 4$ when $n = 4$ and when $n = p^a$, where p is a prime, $p \equiv 3 \pmod 4$.

Proof. If $n = 4$, $\varphi(n) = \varphi(2^2) = 2^2 - 2 = 2 \equiv 2 \pmod 4$. We used Theorem 2.5 in this computation. Let $a \geq 1$ because $\varphi(p^0) = 1 \not\equiv 2 \pmod 4$. If $n = p^a$, where p is prime, $p \equiv 3 \pmod 4$, $\varphi(n) = \varphi(p^a) = p^a - p^{a-1} \equiv 3^a - 3^{a-1} \pmod 4$. Note that

$$\begin{aligned} 3^a &\equiv 1 \pmod 4 \text{ if } a \text{ is even,} \\ 3^a &\equiv 3 \pmod 4 \text{ if } a \text{ is odd.} \end{aligned}$$

Thus

$$\begin{aligned} 3^a - 3^{a-1} &\equiv 3 - 1 \equiv 2 \pmod 4 \text{ if } a \text{ is even,} \\ 3^a - 3^{a-1} &\equiv 1 - 3 \equiv -2 \equiv 2 \pmod 4 \text{ if } a \text{ is odd.} \end{aligned}$$

We have shown that $\varphi(n) \equiv 2 \pmod 4$ when p is a prime such that $p \equiv 3 \pmod 4$. $\square$

Exercise 5.4 (b). Find all n for which $\varphi(n) \equiv 2 \pmod 4$.

Solution. Let us consider the following sets:

- Let $S_1 = \{1\}$.
- Let $S_2 = \{n \mid n = 2^a\}$ for integer $a \geq 1$.
- Let $S_3 = \{n \mid n = p^a m\}$ for prime $p \equiv 1 \pmod 4$, integers $a \geq 1$, $m \geq 1$, $(p, m) = 1$.
- Let $S_4 = \{n \mid n = p^a q^b m\}$ for primes $p \equiv q \equiv 3 \pmod 4$, $p \neq q$, integers $a \geq 1$, $b \geq 1$, $m \geq 1$, $(p, m) = (q, m) = 1$, and $(p', m) = 1$ for all primes $p' \equiv 1 \pmod 4$.
- Let $S_5 = \{n \mid n = p^a 2^b\}$ for prime $p \equiv 3 \pmod 4$ and integers $a \geq 1$, $b \geq 1$.
- Let $S_6 = \{n \mid n = p^a\}$ for prime $p \equiv 3 \pmod 4$ and integer $a \geq 1$.

We now show that every integer n belongs to one of the above sets. First note that every integer has an odd prime factor or it does not. Now consider the following cases:

- If n does not have an odd prime factor, $n \in S_1 \cup S_2$.
- If n has an odd prime factor, the factor is either of the form $4k + 1$ or of the form $4k + 3$ where k is an integer.
  - If n has an odd prime factor of the form $4k + 1$, $n \in S_3$.
  - If n has an odd prime factor but none of the factors is of the form $4k+1$, then all its odd prime factors must be of the form $4k+3$. For such an n, either only a single prime of the form $4k + 3$ divides n or multiple distinct primes of the form $4k + 3$ divide n.

  * If multiple distinct primes of the form $4k+3$ divide n, $n \in S_4$.
  * If only a single prime of the form $4k+3$ divides n, consider that either $2 \mid n$ or $2 \nmid n$.
    - If only a single prime of the form $4k+3$ divides n and $2 \mid n$, $n \in S_5$.
    - If only a single prime of the form $4k+3$ divides n and $2 \nmid n$, $n \in S_6$.

We have shown that $S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5 \cup S_6$ is the set of all integers. We will now find all integers n for which $\varphi(n) \equiv 2 \pmod 4$.

- If $n \in S_1$, i.e., if $n = 1$, then $\varphi(n) = 1 \not\equiv 2 \pmod 4$.
- If $n \in S_2$, i.e., if $n = 2^a$ for integer $a \geq 1$, then $\varphi(n) \equiv 2^{a-1} \pmod 4$. Thus $\varphi(n) = 2 \pmod 4$ if and only if $a = 2$, i.e., $n = 4$.
- If $n \in S_3$, i.e., if $n = p^a m$ for prime $p \equiv 1 \pmod 4$, integers $a \geq 1$, $m \geq 1$, $(p, m) = 1$, then $\varphi(n) = \varphi(p^a)\varphi(m) = (p^a - p^{a-1})\varphi(m) \equiv (1-1)\varphi(m) \equiv 0 \pmod 4$.
- If $n \in S_4$, i.e., if $n = p^a q^b m$ for primes $p \equiv q \equiv 3 \pmod 4$, $p \neq q$, integers $a \geq 1$, $b \geq 1$, $m \geq 1$, $(p, m) = (q, m) = 1$, and $(p', m) = 1$ for all primes $p' \equiv 1 \pmod 4$, then $\varphi(n) = \varphi(p^a)\varphi(q^b)\varphi(m)$. In the solution to part (a) of this exercise problem we have shown that $\varphi(p^a) \equiv 2 \pmod 4$ when prime $p \equiv 3 \pmod 4$ and integer $a \geq 1$. Thus $\varphi(n) \equiv 2 \cdot 2 \cdot \varphi(m) \equiv 0 \not\equiv 2 \pmod 4$.
- If $n \in S_5$, i.e., if $n = p^a 2^b$ for prime $p \equiv 3 \pmod 4$ and integers $a \geq 1$, $b \geq 1$, then $\varphi(n) = \varphi(p^a)\varphi(2^b) \equiv 2 \cdot 2^{b-1} \equiv 2^b \pmod 4$. Thus $\varphi(n) \equiv 2 \pmod 4$ if and only if $b = 1$, i.e., $n = 2p^a$.
- If $n \in S_6$, i.e., if $n = p^a$ for prime $p \equiv 3 \pmod 4$ and integer $a \geq 1$, then $\varphi(n) = \varphi(p^a) \equiv 2 \pmod 4$ as shown in the solution to Exercise 5.4 (a).

We have shown that $\varphi(n) \equiv 2 \pmod 4$ if and only if $n = 4$ or $n = p^a$ or $n = 2p^a$ for prime p and integer $a \geq 1$.

Exercise 5.5. A yardstick is divided into inches is again divided into 70 equal parts. Prove that among the four shortest divisions two have left endpoints corresponding to 1 and 19 inches. What are the right endpoints of the other two?

Solution. TODO

Exercise 5.6. Find all x which simultaneously satisfy the system of congruences

$$x \equiv 1 \pmod 3, \qquad x \equiv 2 \pmod 4, \qquad x \equiv 3 \pmod 5.$$

Solution. From the Chinese remainder theorem shown in Theorem 5.26, we know that there is a unique solution moddulo $3 \cdot 4 \cdot 5 = 60$. Using the method described in the proof of Theorem 5.26, we define the following variables:

$$\begin{aligned}
m_1 &= 3, & b_1 &= 1, & M_1 &= 4 \cdot 5 = 20, & M_1' &= 2, \\
m_2 &= 4, & b_2 &= 2, & M_2 &= 3 \cdot 5 = 15, & M_2' &= 3, \\
m_3 &= 5, & b_3 &= 3, & M_3 &= 3 \cdot 4 = 12, & M_3' &= 3.
\end{aligned}$$

Now we obtain the solution as follows:

$$\begin{aligned}
x &= b_1 M_1 M_1' + b_2 M_2 M_2' + b_3 M_3 M_3' \\
&= 1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 \\
&= 40 + 90 + 108 \\
&= 238 \equiv 58 \pmod{60}.
\end{aligned}$$

Exercise 5.7. Prove the converse of Wilson's theorem: If $(n-1)! + 1 \equiv 0 \pmod n$, then n is prime if $n > 1$.

Proof. We assume n is composite and obtain a contradiction. If n is composite, then $n = cd$ for some integers c and d where $1 < c \leq d < n$. Since $d \mid n$ and $n \mid (n-1)! + 1 \equiv 0$, from the transitive property of divisibility shown in Theorem 1.1 (b), we get $d \mid (n-1)!+1$. Since $1 < d < n$, $d \mid (n-1)!$. Since $d \mid (n-1)! + 1$ and $d \mid (n-1)!$, from the linearity property of divisibility shown in Theorem 1.1 (d), we get $d \mid 1$. Now from the comparison property of divisibility shown in Theorem 1.1 (i), we get $d \leq 1$. This is a contradiction since $d > 1$. $\square$

Exercise 5.8. Find all positive integers n for which $(n-1)! + 1$ is a power of n.

Proof. If $(n-1)!+1 = n^k$ for some integer $k \geq 1$, then $n \mid (n-1)!+1$. By the converse of Wilson's theorem in Exercise 5.7, n is prime. Therefore let $n = p$ for some prime p. Thus $(p-1)! + 1 = p^k$. Subtracting 1 from both sides and dividing both sides by $(p-1)$, we get

$$(p-2)! = \frac{p^k - 1}{p-1}. \tag{1}$$

Now

$$\begin{aligned}\frac{p^k - 1}{p-1} &= p^{k-1} + p^{k-2} + \cdots + p + 1 \\ &= (p^{k-1} - 1) + (p^{k-2} - 2) + \cdots + (p-1) + k \\ &= (p-1)(p^{k-2} + \cdots + 1) + (p-1)(p^{k-3} + \cdots + 1) + \cdots + (p-1) + k.\end{aligned}$$

Therefore

$$\frac{p^k - 1}{p-1} \equiv k \pmod{p-1}. \tag{2}$$

From (1) and (2) we get

$$(p-1)! \equiv k \pmod{p-1}.$$

$\square$

Appendix A

Lemmas

This appendix presents some interesting results in the form of lemmas. These lemmas are used in some of the solutions.

Lemma 1. *The greatest common divisor (gcd) of* a *and* b *is the smallest positive integer that can be written as* $ax + by$ *where* a*,* b*,* x*, and* y *are integers such that either* $a \neq 0$ *or* $b \neq 0$*.*

Proof. Let $d = (a, b)$. From the properties of gcd we know that $d \geq 0$ and in fact $d = 0$ if and only if $a = b = 0$. Since we have either a or b as nonzero, $d > 0$. From the properties of gcd, we know that d can be written as $ax + by$. We will now show that d is the smallest such integer that can be written as $ax + by$.

Assume there exists an integer d' such that $0 < d' < d$ and $d' = ax + by$ for some integers x and y. Then $d \mid d'$ by the linearity property of divisibility. Since $d \mid d'$ and $d' \neq 0$, we get $|d| \leq |d'|$ by the comparison property of divisibility. Since $d \geq 0$ and $d' > 0$, the previous inequality is equivalent to $d \leq d'$. This contradicts our assumption that $d' < d$. $\square$

Lemma 2. *If* $(a, b_1) = (a, b_2) = \cdots = (a, b_n) = 1$*, then* $(a, b_1 b_2 \cdots b_n) = 1$ *where* a*,* b_1*,* b_2*, …,* b_n *are integers.*

Proof. We use induction on n. If $n = 2$, the lemma is true by Exercise 1.2. Assume that the lemma is true for $n - 1$. Therefore $(a, b_1 b_2 \cdots b_{n-1}) = 1$. Since $(a, b_1 b_2 \cdots b_{n-1}) = (a, b_n) = 1$, by Exercise 1.2 we get $(a, b_1 b_2 \cdots b_n) = 1$. $\square$

Lemma 3. *If $(a, b) = 1$, $a \mid c$, and $b \mid c$, then $ab \mid c$ where a, b, and c are integers.*

Proof. Since $a \mid c$, we have $c = ak$ for some integer k. Since $b \mid c$, we have $b \mid ak$. Since $b \mid ak$ and $(b, a) = 1$, by Euclid's lemma we get $b \mid k$. Using the multiplication property of divisibility, we get $ab \mid ak$, i.e., $ab \mid c$. $\square$

Lemma 4. *If $a_1, a_2, \ldots, a_n$ are relatively prime in pairs, $a_1 \mid c$, $a_2 \mid c$, $\ldots$, $a_n \mid c$, then $a_1 a_2 \cdots a_n \mid c$ where $a_1, a_2, \ldots, a_n$, and c are integers.*

Proof. We use induction on n. If $n = 2$, this lemma is true by Lemma ?? of Appendix. Let $A = a_1 a_2 \cdots a_{n-1}$. Assume that this lemma is true for $n - 1$. Therefore $A \mid c$. Since $(a_n, a_1) = (a_n, a_2) = \cdots = (a_n, a_{n-1}) = 1$, using Lemma ?? of Appendix we get $(A, a_n) = 1$. Since $(A, a_n) = 1$, $A \mid c$, and $a_n \mid c$, using the previous lemma we get $Aa_n \mid c$. $\square$

Lemma 5. *Let $m_1, m_2, \ldots, m_r$ are positive integers, relatively prime in pairs. If*

$$\begin{aligned} x &\equiv a \pmod{m_1}, \\ x &\equiv a \pmod{m_2}, \\ &\vdots \\ x &\equiv a \pmod{m_r}, \end{aligned}$$

then $x \equiv a \pmod{m_1 m_2 \cdots m_r}$.

Proof. We have $m_1 \mid (x-a)$, $m_2 \mid (x-a)$, $\ldots$, $m_r \mid (x-a)$, where $m_1, m_2, \ldots, m_r$ are relatively prime in pairs. Therefore, by the previous lemma, we get $m_1 m_2 \cdots m_r \mid (x-a)$, i.e., $x \equiv a \pmod{m_1 m_2 \cdots m_r}$. □

Lemma 6. *If n is composite and $n > 4$, then $n \mid (n-1)!$.*

Proof. If n is composite either n is a square of a prime or it isn't. If $n = p^2$ where p is prime, since $n > 4$, we get $p > 2$. Thus $p^2 - 2p - 1 = 2 \geq 3^2 - 2 \cdot 3 - 1 > 0$, so we get $p^2 - 1 > 2p$. Therefore $(n-1)! = (p^2-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots p \cdots 2p \cdots (2p-1) \cdots (p^2-1)$. Thus $p^2 \mid (n-1)!$ or equivalently $n \mid (n-1)!$.

If $n \neq p^2$ for all primes p, then $n = cd$ for some integers c and d such that $1 < c < d < n$. Thus $(n-1)! = 1 \cdot 2 \cdots c \cdots d \cdots (n-1)$. Thus $cd \mid n$ or equivalently $n \mid (n-1)!$. □