# Number Theory Exam Solutions

**1** Prove that $2^{n+2} \mid (2n+3)!$ for all positive integers $n$.

**Solution.** *We prove this by induction. The statement holds for $k = 1$:*

$$2^{1+2} \mid (2(1)+3)! \implies 8 \mid 120$$

*Assume the statement holds for some arbitrary positive integer $k \geq 1$. That is, assume:*

$$2^{k+2} \mid (2k+3)!$$

*This implies that $(2k+3)! = m \cdot 2^{k+2}$ for some integer $m$.*

*We now prove:*

$$2^{(k+1)+2} \mid (2(k+1)+3)! \implies 2^{k+3} \mid (2k+5)!$$

*We have*

$$\begin{aligned}(2k+5)! &= (2k+5)\cdot(2k+4)\cdot(2k+3)! \\ &= (2k+5)\cdot(2k+4)\cdot(m\cdot 2^{k+2}) \quad \textit{(by Inductive Hypothesis)} \\ &= [(2k+5)(k+2)m]\cdot 2^{k+3}\end{aligned}$$

*Let $j = (2k+5)(k+2)m$. Since $k$ and $m$ are integers, $j$ is an integer. Therefore, $(2k+5)! = j \cdot 2^{k+3}$, which shows that $2^{k+3} \mid (2k+5)!$. This is precisely the statement for $k+1$.*

**2** Let $a, b, c$ be integers. If $\gcd(a,b) = 1$ and $c \mid (a+b)$, then show that $\gcd(a,c) = 1$.

**Solution.** *Let $d = \gcd(a,c)$. Then $d \mid a$ and $d \mid c$. Since $c \mid (a+b)$, we have $d \mid (a+b)$ as well. Since $d \mid a$ and $d \mid (a+b)$, it follows that $d \mid ((a+b)-a) = b$. Hence $d$ divides both $a$ and $b$, so $d \mid \gcd(a,b) = 1$. Thus $d = 1$, i.e. $\gcd(a,c) = 1$.*

***Alternative solution:*** *As $\gcd(a,b) = 1$ by Bezout's there exist $x, y \in \mathbb{Z}$ such that $ax+by = 1$. Moreover by the assumption we have $a+b = ck$. So we get $b = ck - a$ which gives*

$$1 = ax + by = ax + (ck-a)y = a(x-y) + c(yk)$$

*So we get $\gcd(a,c) = 1$.*

**3** **(a)** For which values of $k$ does the equation $123x + 360y = k$ have at least one integer solution?

**Solution.** *A linear equation $ax + by = k$ has an integer solution iff $\gcd(a, b) \mid k$. We compute $\gcd(123, 360)$ using the Euclidean algorithm:*

$$\begin{aligned} 360 &= 2 \cdot 123 + 114 \\ 123 &= 1 \cdot 114 + 9 \\ 114 &= 12 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

*Thus $\gcd(123, 360) = 3$. Therefore the equation has an integer solution exactly for those integers $k$ that are multiples of 3, i.e. $k \in 3\mathbb{Z}$.*

**(b)** Solve the linear congruence $360x \equiv 99 \pmod{123}$, or explain why no solutions exist.

**Solution.** *First note $\gcd(360, 123) = 3$ (from part (a)). Since $3 \mid 99$, solutions exist. Divide the congruence by 3:*

$$120x \equiv 33 \pmod{41}.$$

*We have $120 \equiv 38 \equiv -3 \pmod{41}$ and its inverse is $-14 \bmod 41$. So multiply both sides by $-14$:*

$$x \equiv -14 \cdot 33 \equiv 30 \pmod{41}.$$

*Therefore all solutions in $\mathbb{Z}/123\mathbb{Z}$ are*

$$\overline{30}, \overline{71} \text{ and } \overline{112}.$$

**4** A *Carmichael number* is an odd composite number $n$ which satisfies $a^{n-1} \equiv 1 \pmod{n}$ for every integer $a$ with $\gcd(a, n) = 1$. Show that $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number.

**Solution.** *We will show that* $a^{560} \equiv 1$ *modulo each prime factor. Since the moduli* 3, 11, *and* 17 *are pairwise coprime, then we will have* $a^{560} \equiv 1 \mod 561$ *by applying Theorem 7.12-(2) t pairs* $(3, 11)$ *and* $(33, 17)$.

*By Fermat's Little Theorem, since* 3 *is prime and* $\gcd(a, 3) = 1$, *we have* $a^{3-1} \equiv a^2 \equiv 1 \pmod{3}$. *So we get*

$$a^{560} = a^{2 \cdot 280} = (a^2)^{280} \equiv (1)^{280} \equiv 1 \pmod{3}$$

*By Fermat's Little Theorem, since* 11 *is prime and* $\gcd(a, 11) = 1$, *we have* $a^{11-1} \equiv a^{10} \equiv 1 \pmod{11}$. *So we have*

$$a^{560} = a^{10 \cdot 56} = (a^{10})^{56} \equiv (1)^{56} \equiv 1 \pmod{11}$$

*By Fermat's Little Theorem, since* 17 *is prime and* $\gcd(a, 17) = 1$, *we have* $a^{17-1} \equiv a^{16} \equiv 1 \pmod{17}$. *So we have*

$$a^{560} = a^{16 \cdot 35} = (a^{16})^{35} \equiv (1)^{35} \equiv 1 \pmod{17}$$

**5** **(a)** State Fermat's theorem.

**Solution.** *If $p$ is a prime number and $p \nmid a$, then $p|(a^{p-1}-1)$.*

**(b)** Let $p$ and $q$ be distinct primes and let $a$ be an integer such that $\gcd(a, pq) = 1$. If

$$a^p \equiv a \pmod{q} \qquad \text{and} \qquad a^q \equiv a \pmod{p},$$

then show that $a^{pq} \equiv a \pmod{pq}$.

**Solution.** *Since* $\gcd(a, pq) = 1$*, we have* $\gcd(a, p) = \gcd(a, q) = 1$*. By Fermat's little theorem,*

$$a^{p-1} \equiv 1 \pmod{p} \quad \textit{and} \quad a^{q-1} \equiv 1 \pmod{q}.$$

*This gives*

$$a^p \equiv a \pmod{p} \quad \textit{and} \quad a^q \equiv a \pmod{q}.$$

*Consider $a^{pq}$ modulo $p$:*

$$a^{pq} \equiv (a^q)^p \equiv a^p \equiv a \pmod{p}.$$

*Similarly modulo $q$,*

$$a^{pq} \equiv (a^p)^q \equiv a^q \equiv a \pmod{q}.$$

*Since $p$ and $q$ are distinct primes and both divides $a^{pq} - a$ by Theorem 7.12-(2) we have*

$$a^{pq} \equiv a \pmod{pq}.$$

**6** For each of the following statements, prove it if it is correct, and disprove it if it is incorrect.

**(a)** If $m$ is a positive integer and $a^2 \equiv b^2 \pmod{m}$, then $a \equiv b \pmod{m}$ or $a \equiv -b \pmod{m}$.

**Solution.** *A counterexample is* $m = 8$, $a = 1$, $b = 3$*:*

$$1^2 = 1, \quad 3^2 = 9 \equiv 1 \pmod{8},$$

*so* $a^2 \equiv b^2 \pmod{8}$*, but* $1 \not\equiv 3 \pmod{8}$ *and* $1 \not\equiv -3 \pmod{8}$*.*

**(b)** $\{\, 5x + 12y + 8z \mid x, y, z \in \mathbb{Z} \,\} = \mathbb{Z}$.

**Solution.** *This statement is* true*. As we have* $\gcd(5, 12) = 1$*, there exist* $x, y \in \mathbb{Z}$ *such that* $5x + 12y = 1$*. So we have* $5x + 12y = k$ *with* $k \in \mathbb{Z}$ *as* $1 \mid k$*. So we get*

$$\{5x + 12y + 8z\} = \{k + 8z\}$$

*and as* $\gcd(1, 8) = 1$ *we have* $k + 8z = t$ *(as* $1 \mid t$*) for any integer* $t$*. So we get*

$$\{5x + 12y + 8z\} = \{k + 8z\} = \{t \mid t \in \mathbb{Z}\}.$$

**(c)** $2^{11} + 1$ divides $2^{66} + 1$.

**Solution.** *The statement is* false*. The claim would mean* $2^{11} + 1$ *divides* $2^{66} + 1$*. On the other hand, reducing modulo* $2^{11} + 1$ *we have* $2^{11} \equiv -1$*, hence*

$$2^{66} + 1 \equiv (-1)^6 + 1 = 1 + 1 = 2 \pmod{2^{11} + 1}.$$

*So not dividing.*

**(d)** Over $\mathbb{Z}/39\mathbb{Z}$ the matrix equation $\begin{bmatrix} \overline{5} & \overline{3} \\ \overline{3} & \overline{12} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \overline{4} \\ \overline{5} \end{bmatrix}$ has a unique solution.

**Solution.** *The system has a unique solution iff the determinant is a unit in* $\mathbb{Z}/39\mathbb{Z}$*. The determinant*

$$\det \begin{bmatrix} \overline{5} & \overline{3} \\ \overline{3} & \overline{12} \end{bmatrix} = \overline{51}$$

*which is not a unit as* $\gcd(51, 39) = 3 \neq 1$.

**Bonus.** For distinct primes $p$ and $q$, show that

$$\varphi(p^e q^f) \;=\; \varphi(p^e)\,\varphi(q^f)$$

for any positive integers $e$ and $f$, where $\varphi$ denotes Euler's totient function.

**Solution.** *We have*

$$\begin{aligned}
\varphi(p^e q^f) &= p^e q^f - p^{e-1} q^f - p^e q^{f-1} - p^{e-1} q^{f-1} \\
&= q^f (p^e - p^{e-1}) - q^{f-1}(p^e - p^{e-1}) \\
&= (q^f - q^{f-1})(p^e - p^{e-1}) \\
&= \varphi(q^f)\varphi(p^e)
\end{aligned}$$