CS215: Discrete Math (H)
2023 Fall Semester Written Assignment # 3
Due: Nov. 13th, 2023, please submit at the beginning of class

Q.1 What are the prime factorizations of

(a) 12!

(b) 6560

Solution:

(a) $12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$.

(b) $6560 = 2^5 \cdot 5 \cdot 41$.

$\square$

Q.2

(a) Give the prime factorization of 312.

(b) Use Euclidean algorithm to find $\gcd(312, 97)$.

(c) Find integers s and t such that $\gcd(312, 97) = 312s + 97t$.

(d) Solve the modular equation

$$312x \equiv 3 \pmod{97}.$$

Solution:

(a) The prime factorization is $312 = 2^3 \cdot 3 \cdot 13$.

(b) Applying Euclidean algorithm, we have

$$\begin{aligned}
\gcd(312, 97) &= \gcd(97, 21) \quad [312 = 3 \cdot 97 + 21] \\
&= \gcd(21, 13) \quad [97 = 4 \cdot 21 + 13] \\
&= \gcd(13, 8) \quad [21 = 1 \cdot 13 + 8] \\
&= \gcd(8, 5) \quad [13 = 1 \cdot 8 + 5] \\
&= \gcd(5, 3) \quad [8 = 1 \cdot 5 + 3] \\
&= \gcd(3, 2) \quad [5 = 1 \cdot 3 + 2] \\
&= \gcd(2, 1) \quad [3 = 1 \cdot 2 + 1] \\
&= 1.
\end{aligned}$$

(c) Reading Euclidean algorithm backwards we have

$$1 = 37 \cdot 312 - 119 \cdot 97.$$

(d) So $312 \cdot 37 \equiv 1 \pmod{97}$. Thus, $312 \cdot (37 \cdot 3) \equiv 3 \pmod{97}$. Now $37 \cdot 3 = 111 \equiv 14 \pmod{97}$. Hence, the solution is $x \equiv 14 \pmod{97}$.

$\square$

Q.3 Prove the following statement: Suppose that $\gcd(b, a) = 1$. Prove that $\gcd(b + a, b - a) \leq 2$.
Solution: W.l.o.g., assume that $b \geq a$. Now suppose that $d|(b + a)$ and $d|(b - a)$. Then $d|[(b + a) + (b - a)] = 2b$ and $d|[(b + a) - (b - a)] = 2a$. Thus, we have

$$d|\gcd(2b, 2a) = 2\gcd(b, a) = 2.$$

Therefore, we have $d \leq 2$.

$\square$

Q.4 Prove that there exist two powers of 2 that differ by a multiple of 222. That is, prove that there exist two positive integers x and y, such that 222 divides $2^y - 2^x$.

Solution: We prove this by the pigeonhole principle. Let $a_n = 2^n \bmod 222$. By the definition of modular arithmetic, $0 \leq a_n \leq 221$. Since a_n is an infinite sequence but can only take finitely many values, there must be m and n such that $a_n = a_m$ and therefore $2^n \equiv 2^m \bmod 222$, and further we have $2^n - 2^m \equiv 0 \bmod 222$.

Q.5 Given an integer a, we say that a number n passes the "Fermat primality test (for base a)" if $a^{n-1} \equiv 1 \pmod{n}$.

(a) For $a = 2$, does $n = 561$ pass the test?

(b) Did the test give the correct answer in this case?

Solution:

(a) We have

$$\begin{aligned}
2^{560} &\equiv 2^{20\cdot 28} \pmod{561} \\
&\equiv (2^{20})^{28} \pmod{561} \\
&\equiv (67)^{28} \pmod{561} \\
&\equiv (67^4)^7 \pmod{561} \\
&\equiv 1^7 \pmod{561} \\
&\equiv 1.
\end{aligned}$$

Thus, $2^{560} \equiv 1 \pmod{561}$. So 561 passes the Fermat test with test value 2.

(b) We have $561 = 3 \cdot 11 \cdot 17$. So, 561 is not a prime, and thus the test failed.

□

Q.6 Let a and b be positive integers. Show that $\gcd(a,b) + \operatorname{lcm}(a,b) = a + b$ if and only if a divides b, or b divides a.
Solution:

"only if" Assume that $\gcd(a,b) = d$, then we have $\operatorname{lcm}(a,b) = \frac{ab}{d}$, where d is an integer. Then we have $d + \frac{ab}{d} = a + b$, and we further have $d^2 - (a+b)d + ab = 0$, Solving this equation, we have $d = a$ or $d = b$. This means a divides b or b divides a.

"if" W.l.o.g., assume that $a|b$. Then we have $\gcd(a,b) = a$ and $\operatorname{lcm}(a,b) = b$. The conclusion then follows.

□

Q.7

(1) Show that there is no integer solution x to the equation

$$x^2 \equiv 31 \pmod{36}.$$

(2) Find the integer solutions x to the system of equations

$$\begin{cases} x^2 \equiv 10 \pmod{31}, \\ x^2 \equiv 30 \pmod{37}. \end{cases}$$

Solution:

(1) Note that $36 = 4 \cdot 9$. If x is a solution to the equation, then we also have that

$$\begin{aligned} x^2 &\equiv 31 \equiv 3 \pmod 4, \\ x^2 &\equiv 31 \equiv 4 \pmod 9. \end{aligned}$$

Yet, there is no x such that $x^2 \equiv 3 \pmod 4$. Hence there is no solution to this equation.

(2) Let $y = x^2$. Since $y \equiv 30 \pmod{37}$, we have that

$$y = 30 + 37k$$

for some integer k. The first equation becomes

$$30 + 37k \equiv 10 \pmod{31} \Leftrightarrow 6k \equiv -20 \equiv 11 \pmod{31}.$$

To solve this equation, we note that

$$31 = 5 \cdot 6 + 1 \Rightarrow (-5) \cdot 6 \equiv 1 \pmod{31}.$$

Hence, we have

$$(-5) \cdot 6k \equiv (-5) \cdot 11 \pmod{31} \Leftrightarrow k \equiv -55 \equiv 7 \pmod{31}.$$

As a consequence, k is of the form $7 + 31m$ for some integer m, which yields that

$$\begin{aligned} x^2 = y &= 30 + 37(7 + 31m) \\ &= 30 + 37 \cdot 7 + 37 \cdot 31m \\ &= 289 + 1147m = 17^2 + 1147m. \end{aligned}$$

Choosing $m = 0$, we obtain that $x = 17, -17$ are the integer solutions.

Q.8 Prove that if a and m are positive integers such that $\gcd(a, m) \neq 1$ then a does *not* have an inverse modulo m.

Solution: We prove this by contrapositive. Assume that a has an inverse modulo m, i.e., there exists an integer b such that

$$ab \equiv 1 \pmod m.$$

This is equivalent to $m|(ab-1)$, which means that there is an integer k such that

$$ab - 1 = mk,$$

which is

$$ba + (-k)m = 1.$$

Suppose that d is any common divisor of a and m, i.e., $d|a$ and $d|m$. Since b and k are integers, it follows that $d|(ba - km)$, so $d|1$. Thus, we must have $d = 1$, which completes the proof.

□

Q.9 Convert the decimal expansion of each of these integers to a binary expansion.

(a) 321 (b) 1023 (c) 100632

Solution: (a) 101000001

(b) 1111111111

(c) 11000100100011000

□

Q.10 Suppose that p, q and r are distinct primes. Show that there exist integers a, b and c, such that

$$a(pq) + b(qr) + c(rp) = 1.$$

Solution: Since p, q and r are distinct primes, we have $\gcd(p, r) = 1$ and by Bezout's theorem, we have $1 = sp + tr$ and further $s(pq) + t(qr) = q$. Now by $\gcd(q, rp) = 1$, so there exist integers u and v such that

$$uq + v(rp) = 1.$$

Therefore, we have

$$u(s(pq) + t(qr)) + v(rp) = (us)(pq) + (ut)(qr) + v(rp) = 1.$$

□

Q.11 From Google's Corporate Information Page:
"1997 – Larry (Page) and Sergey (Brin) decide that the BackRub search engine needs a new name. After some brainstorming, they go with Google – a play on the word ' googol', a mathematical term for the number represented by the numeral 1 followed by 100 zeros. The use of the term reflects their mission to organize a seemingly infinite amount of information on the web."

The name ' googol' for 10^{100} was coined (around 1920) by a nine-year old child. He also called 10^{googol} a ' googolplex'. Accordingly, Googleplex is the name of Google's headquarters complex in California.

What is the remainder of a googol to a googol modulo 13, i.e., $(10^{100})^{(10^{100})} \bmod 13$?

Solution:

By Fermat's little theorem, we have $10^{12} \equiv 1 \pmod{13}$. Thus, we have

$$10^{100} \equiv 10^{12 \cdot 8+4} \equiv 10^4 \equiv 3 \pmod{13}.$$

It then follows that

$$(10^{100})^{(10^{100})} \bmod 13 = 3^{(10^{100})} \bmod 13.$$

Note that $3^3 \equiv 1 \pmod{13}$. It is also easily seen that $10^{100} \equiv 1 \pmod 3$, which leads to $10^{100} = 3k+1$ for an integer k. Therefore, we have

$$(10^{100})^{(10^{100})} \bmod 13 = 3^{(10^{100})} \bmod 13 = 3^{3k+1} \bmod 13 = 3.$$

□

Q.12 Let the coefficients of the polynomial $f(n) = a_0 + a_1 n + a_2 n^2 + \cdots + a_{t-1} n^{t-1} + n^t$ be integers. We now show that ***no*** non-constant polynomial can generate only prime numbers for integers n. In particular, let $c = f(0) = a_0$ be the constant term of f.

(1) Show that $f(cm)$ is a multiple of c for all $m \in \mathbb{Z}$.

(2) Show that if f is non-constant and $c > 1$, then as n ranges over the nonnegative integers $\mathbb{N}$, there are infinitely many $f(n) \in \mathbb{Z}$ that are not primes. [Hint: You may assume the fact that the magnitude of any non-constant polynomial $f(n)$ grows unboundedly as n grows.]

(3) Conclude that for every non-constant polynomial f there must be an $n \in \mathbb{N}$ such that $f(n)$ is not prime. [Hint: Only one case remains.]

Solution:

(1) Let $f(n) = g(n) + c$, where $g(n)$ has no constant term. Then we have $f(cm) = g(cm) + c$. Since $g(n)$ has no constant term, $g(cm)$ must have a divisor cm. Thus, c must be a divisor of $f(cm)$.

(2) Since as $n = cm$ grows, the magnitude of $f(n)$ grows unboundedly, and $f(n)$ is composite with a divisor $c > 1$. Thus, there are infinitely many $f(n)$ that are not primes.

(3) The only one remaining case is $c = 1$. Since the degree of $f(n)$ is t, by replacing n by $n+a$ for $t+1$ different values of a, we must have at least one of them such that the constant term of $g(n+a)$ is nonzero. Suppose this value of a is n_0. Let $h(n) = f(n + n_0)$, and let $d = h(0)$. Then $d > 1$. By (1), we have $h(dm)$ is always a multiple of d. Therefore, with $n = dm - n_0$, $f(n)$ is not prime.

$\square$

Q.13 Show that $\log_2 3$ is an irrational number. Recall that an irrational number is a real number x cannot be written as the ratio of two integers.
Solution: Suppose that $\log_2 3 = a/b$ where $a, b \in \mathbf{Z}^+$ and $b \neq 0$. Then $2^{a/b} = 3$, so $2^a = 3^b$. This violates the fundamental theorem of arithmetic. Hence $\log_2 3$ is irrational.

$\square$

Q.14 Show that if a and m are relatively prime positive integers, then the inverse of a modulo m is unique modulo m.
Solution:

Suppose that b and c are both the inversed of a modulo m. Then $ba \equiv 1 \pmod{m}$ and $ca \equiv 1 \pmod{m}$. Hence, $ba \equiv ca \pmod{m}$. Because $\gcd(a, m) = 1$ it follows by Theorem 7 in Section 4.3 that $b \equiv c \pmod{m}$.

$\square$

Q.15 Prove that there are infinitely many primes of the form $4k+3$, where k is a nonnegative integer. [Hint: Suppose that there are only finitely many such primes $q_1, q_2, \dots, q_n$, and consider the number $4q_1q_2\cdots q_n - 1$.]

Solution: Suppose that there are only finitely many primes of the form $4k+3$, namely $q_1, q_2, \dots, q_n$, where $q_1 = 3$, $q_2 = 7$, and so on.

Let $Q = 4q_1q_2\cdots q_n - 1$. Note that Q is of the form $4k+3$ (where $k = q_1q_2\cdots q_n - 1$). If Q is prime, then we have found a prime of the desired form different from all those listed.

If Q is not prime, then Q has at least one prime factor not in the list $q_1, q_2, \dots, q_n$, because the remainder when Q is divided by q_j is $q_j - 1$, and $q_j - 1 \neq 0$. Because all odd primes are either of the form $4k+1$ or of the form $4k+3$, and the product of primes of the form $4k+1$ is also of this form (because $(4k+1)(4m+1) = 4(4km+k+m)+1$), there must be a factor of Q of the form $4k+3$ different from the primes we listed.

$\square$

Q.16

(a) Use Fermat's little theorem to compute 5^{2003} mod 7, 5^{2003} mod 11, and 5^{2003} mod 13.

(b) Use your results from part (a) and the Chinese remainder theorem to find 5^{2003} mod 1001. (Note that $1001 = 7 \cdot 11 \cdot 13$.)

Solution:

(a) By Fermat's little theorem we know that $5^6 \equiv 1 \pmod 7$; therefore $5^{1998} = (5^6)^{333} \equiv 1^{75} \equiv 1 \pmod 7$, and so $5^{2003} = 5^5 \cdot 5^{1998} \equiv 3 \cdot 1 = 3 \pmod 7$, so $5^{2003} \bmod 7 = 3$. Similarly, $5^{10} \equiv 1 \bmod 11$; therefore $5^{2000} = (5^{10})^{200} \equiv 1 \pmod{11}$, and so $5^{2003} = 5^3 \cdot 5^{2000} \equiv 4 \pmod{11}$, so $5^{2003} \bmod 11 = 4$. Finally, $5^{12} \equiv 1 \pmod{13}$; therefore $5^{1992} = (5^{12})^{166} \equiv 1 \pmod{13}$, and so $5^{2003} = 5^{11} \cdot 5^{1992} \equiv 8 \pmod{13}$, so $5^{2003} \bmod 13 = 8$.

(b) 983

$\square$

Q.17 Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime integers greater than or equal to 2. Show that if $a \equiv b \pmod{m_i}$ for $i = 1, 2, \ldots, n$, then $a \equiv b \pmod{m}$, where $m = m_1 m_2 \cdots m_n$.

Solution:

Suppose that p is a prime appearing in the prime factorization of $m_1 m_2 \cdots m_n$. Because the m_i's are relatively prime, p is a factor of exactly one of the m_i's, say m_j. Because m_j divides $a - b$, it follows that $a - b$ has the factor p in its prime factorization to a power at least as large as the power to which it appears in the prime factorization of m_j. It follows that $m_1 m_2 \cdots m_n$ divides $a - b$, so $a \equiv b \pmod{m_1 m_2 \cdots m_n}$.

□

Q.18 Show that the simultaneous solution of a system of linear congruences modulo pairwise relatively prime moduli is *unique* modulo the product of these moduli.

Solution: Suppose that there are two solutions to the system of linear congruences. Thus, suppose that $x \equiv a_i \pmod{m_i}$ and $y \equiv a_i \pmod{m_i}$ for all i. We want to show that these solutions are the same modulo m. This will guarantee that there is only one nonnegative solution less than m. The assumption certainly implies that $x \equiv y \pmod{m_i}$ for all i. But then the previous problem tells us that $x \equiv y \pmod{m}$, as desired.

□

Q.19 Find all solutions, if any, to the system of congruences $x \equiv 5 \pmod{6}$, $x \equiv 3 \pmod{10}$, and $x \equiv 8 \pmod{15}$.

Solution:

We cannot apply the Chinese remainder theorem directly, since the moduli are not pairwise relatively prime. However, we can using the Chinese remainder theorem, translate these congruences into a set of congruences that together are equivalent to the given congruence. Since we want $x \equiv 5 \pmod{6}$, we must have $x \equiv 5 \equiv 1 \pmod{2}$ and $x \equiv 5 \equiv 2 \pmod{3}$. Similarly, fromt he second congruence we must have $x \equiv 1 \pmod{2}$ and $x \equiv 3 \pmod{5}$; and from the third congruence we must have $x \equiv 2 \pmod{3}$ and $x \equiv 3 \pmod{5}$. Since these six statements are consistent, we see that our system is equivalent to the system $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 3$

(mod 5). These can be solved using the Chinese remainder theorem to yield $x \equiv 23 \pmod{30}$. Therefore the solutions are all integers of the form $23+30k$, where k is an integer.

□

Q.20 Recall how the *linear congruential method* works in generating pseudorandom numbers: Initially, four parameters are chosen, i.e., the modulus m, the multiplier a, the increment c, and the seed x_0. Then a sequence of numbers $x_1, x_2, \ldots, x_n, \ldots$ are generated by the following congruence

$$x_{n+1} = (ax_n + c) \pmod{m}.$$

Suppose that we know the generated numbers are in the range $0, 1, \ldots, 10$, which means the modulus $m = 11$. By observing three consecutive numbers $7, 4, 6$, can you predict the next number? Explain your answer.

Solution: By the linear congruential method, we know that

$$\begin{aligned} x_{n+2} &= (ax_{n+1} + c) \pmod{m} \\ x_{n+1} &= (ax_n + c) \pmod{m}. \end{aligned}$$

Then we have

$$x_{n+2} - x_{n+1} \equiv a(x_{n+1} - x_n) \pmod{m}.$$

By the three consecutive numbers $7, 4, 6$, we then have

$$\begin{aligned} &(1) \quad 6 - 4 \equiv a(4 - 7) \pmod{11}, \\ &(2) \quad x - 6 \equiv a(6 - 4) \pmod{11}, \end{aligned}$$

where x denotes the next number. Eq. (1) gives $8a \equiv 2 \pmod{11}$, and we further have $a \equiv 3 \pmod{11}$. Then by Eq. (2), we have $x \equiv 6 + 3 \cdot 2 \equiv 1 \pmod{11}$. This means the next number is 1.

□

Q.21 Recall that Euler's totient function $\phi(n)$ counts the number of positive integers up to a given integer n that are coprime to n. Let $m, n \geq 2$ be positive integers such that $m|n$. Prove that $\phi(m)|\phi(n)$ and that $\phi(mn) = m\phi(n)$.

Solution: Since $m|n$, by the fundamental theorem of arithmetic, we have

$$m = p_1^{a_1} \cdots p_s^{a_s}, \quad n = p_1^{b_1} \cdots p_s^{b_s} p_{s+1}^{b_{s+1}} \cdots p_t^{b_t},$$

where $t \geq s$, $0 < a_i \leq b_i$ for $i = 1, 2, \ldots, s$ and $0 < b_i$ for $i > s$, and $p_1, \ldots, p_t$ are pairwise distinct prime numbers.

Now, we have

$$\phi(m) = (p_1 - 1)p_1^{a_1-1} \cdots (p_s - 1)p_s^{a_s-1},$$

and

$$\phi(n) = (p_1 - 1)p_1^{b_1-1} \cdots (p_s - 1)p_s^{b_s-1}(p_{s+1} - 1)p_{s+1}^{b_{s+1}-1} \cdots (p_t - 1)p_t^{b_t-1}.$$

It is then clear that $\phi(m)|\phi(n)$. Furthermore, since $mn = p_1^{a_1+b_1} \cdots p_s^{a_s+b_s} p_{s+1}^{b_{s+1}} \cdots p_t^{b_t}$, and

$$\phi(mn) = (p_1-1)p_1^{a_1+b_1-1} \cdots (p_s-1)p_s^{a_s+b_s-1}(p_{s+1}-1)p^{b_{s+1}-1} \cdots (p_t-1)p_t^{b_t-1} = m\phi(n).$$

[Alternative] Suppose that the result is false and let $m|n$ be a counterexample with the *smallest* possible n. Let p be a prime divisor of m. Thus, we can write $m = p^a m_1$ and $n = p^b n_1$ for some $0 < a \leq b$ and natural numbers n_1, m_1 not divisible by p. Since $m_1|m$ and $m|n$, then we have $m_1|n = p^b n_1$. And by $\gcd(p, m_1) = 1$, we have $m_1|n_1$. By the property of the Euler's totient function, we have

$$\phi(m) = \phi(p^a)\phi(m_1) = (p - 1)p^{a-1}\phi(m_1),$$
$$\phi(n) = \phi(p^b)\phi(n_1) = (p - 1)p^{b-1}\phi(n_1),$$

and

$$\phi(mn) = \phi(p^{a+b})\phi(m_1 n_1) = (p - 1)p^{a+b-1}\phi(m_1 n_1).$$

Since $m_1|n_1$ and $n_1 < n$, the result if true for m_1, n_1, i.e., $\phi(m_1)|\phi(n_1)$ and $\phi(m_1 n_1) = m_1\phi(n_1)$. However, we then have

$$\phi(m) = (p - 1)p^{a-1}\phi(m_1)|(p - 1)p^{b-1}\phi(m_1)|(p - 1)p^{b-1}\phi(n_1) = \phi(n),$$

and

$$\phi(mn) = (p - 1)p^{a+b-1}\phi(m_1 n_1) = p^a m_1(p - 1)p^b\phi(n_1) = m\phi(n).$$

Therefore, the result if true for m, n, contradicting to our assumption. The proof is completed.

$\square$

Q.22 Show that we can easily factor n when we know that n is the product of two primes, p and q, and we know the value of $(p-1)(q-1)$.
Solution: Suppose that we know both $n = pq$ and $(p-1)(q-1)$. To find p and q, first note that $(p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$. From this we can find $s = p+q$. Then with $n = pq$, we can use the quadratic formula to find p and q.

$\square$

Q.23 Consider the RSA encryption method. Let our public key be $(n, e) = (65, 7)$, and our private key be d.

(a) What is the encryption $\hat{M}$ of a message $M = 8$?

(b) To decrypt, what value d do we need to use?

(c) Using d, run the RSA decryption method on $\hat{M}$.

Solution:

(a) To encrypt $M = 8$, we have

$$\begin{aligned}
\hat{M} &= M^e \bmod n \\
&= 8^7 \bmod 65 \\
&= 8^{2\cdot 3+1} \bmod 65 \\
&= 64^3 \cdot 8 \bmod 65 \\
&= (-1)^3 \cdot 8 \bmod 65 \\
&= -8 \bmod 65 \\
&= 57 \bmod 65.
\end{aligned}$$

So the encrypted message is $\hat{M} = 57$.

(b) Recall we can find d by running Euclidean algorithm.

$$\begin{aligned}
\gcd(\phi(n), e) &= \gcd(48, 7) & \\
&= \gcd(7, 6) & \text{as } 48 = 6 \cdot 7 + 6 \\
&= \gcd(6, 1) & \text{as } 7 = 1 \cdot 6 + 1 \\
&= 1. &
\end{aligned}$$

Thus $d = \gcd(48, 7) = 1$. Reading backwards we get $1 = 7 \cdot 7 - 1 \cdot 48$. Then the private key $d = 7$.

(c) To complete the RSA decryption, we calculate

$$\begin{aligned} \hat{M}^d \bmod n &= 57^7 \bmod 65 \\ &= (-8)^7 \bmod 65 \\ &= (-8)^{2\cdot 3+1} \bmod 65 \\ &= (64)^3 \cdot (-8) \bmod 65 \\ &= 8 \bmod 65. \end{aligned}$$

Therefore, the original message is $M = 8$ as desired.

$\square$

Q. 24 Consider the RSA system. Let (e, d) be a key pair for the RSA. Define

$$\lambda(n) = \operatorname{lcm}(p-1, q-1)$$

and compute $d' = e^{-1} \bmod \lambda(n)$. Will decryption using d' instead of d still work? (prove $C^{d'} \bmod n = M$)

Solution: <u>Case `I`:</u> $\gcd(M, n) = 1$.

$$\begin{aligned} C^{d'} \bmod n &= M^{ed'} \bmod n = M^{k\lambda(n)+1} \bmod n \\ &= (M^{k\lambda(n)} \bmod n) M \bmod n \\ &= \left(M^{(p-1)(q-1)/\gcd(p-1,q-1)} \bmod n\right)^k M \bmod n \end{aligned}$$

By Fermat's theorem, $M^{(p-1)(q-1)/\gcd(p-1,q-1)} \bmod p = \left(M^{(q-1)/\gcd(p-1,q-1)}\right)^{p-1} \bmod p = 1$ and $M^{(p-1)(q-1)/\gcd(p-1,q-1)} \bmod q = 1$. Then by Chinese Remainder Theorem, we have $C^{d'} \bmod n = M$.

<u>Case `II`:</u> $\gcd(M, n) = p$. $M = tp$ for some integer $0 < t < q$. We have $\gcd(M, q) = 1$ and $ed' = k\lambda(n) + 1$ for some integer k. By Fermat's theorem, we have

$$(M^{k\lambda(n)} - 1) \bmod q = (M^{k(p-1)(q-1)/\gcd(p-1,q-1)} - 1) \bmod q = 0.$$

Then

$$\begin{aligned} (M^{ed'} - M) \bmod n &= M(M^{ed'-1} - 1) \bmod n \\ &= tp(M^{k\lambda(n)} - 1) \bmod pq \\ &= 0 \end{aligned}$$

Case `III`: $\gcd(M, n) = q$. Similar to Case II.
Case `IV`: $\gcd(M, n) = pq$. Trivial.

$\square$