CS215: Discrete Math (H)
2022 Fall Semester   Written Assignment # 3
Due: Nov. 4th, 2022, please submit at the beginning of class

Q.1 What are the prime factorizations of

(a) 8085

(b) 497

(c) 10!

Solution:

(a) $8085 = 3 \cdot 5 \cdot 7^2 \cdot 11$.

(b) $497 = 7 \cdot 71$.

(c) $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$.

$\square$

Q.2

(a) Use Euclidean algorithm to find $\gcd(267, 79)$.

(b) Find integers s and t such that $\gcd(267, 79) = 79s + 267t$.

(c) Solve the modular equation $267x \equiv 3 \pmod{79}$.

Solution:

(a) By Euclidean algorithm, we have

$$\begin{aligned} 267 &= 3 \cdot 79 + 30 \\ 79 &= 2 \cdot 30 + 19 \\ 30 &= 1 \cdot 19 + 11 \\ 19 &= 1 \cdot 11 + 8 \\ 11 &= 1 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Thus, $\gcd(267, 79) = 1$.

(b) By (a), we have

$$\begin{aligned}
1 &= 3-2 \\
&= 3-(8-2\cdot 3) \\
&= 3\cdot 3-8 \\
&= 3\cdot(11-8)-8 \\
&= 3\cdot 11-4\cdot 8 \\
&= 3\cdot 11-4\cdot(19-11) \\
&= 7\cdot 11-4\cdot 19 \\
&= 7\cdot(30-19)-4\cdot 19 \\
&= 7\cdot 30-11\cdot 19 \\
&= 7\cdot 30-11\cdot(79-2\cdot 30) \\
&= 29\cdot 30-11\cdot 79 \\
&= 29\cdot(267-3\cdot 79)-11\cdot 79 \\
&= 29\cdot 267-98\cdot 79.
\end{aligned}$$

(c) By (b), we know that $29\cdot 267 \equiv 1 \pmod{79}$. Thus, we have $x \equiv 29\cdot 3 \equiv 87 \equiv 8 \pmod{79}$.

$\square$

Q.3 Prove the following statements.

(a) If $c|(a\cdot b)$, then $c|(a\cdot \gcd(b,c))$.

(b) Suppose that $\gcd(a,y)=d_1$ and $\gcd(b,y)=d_2$. Prove that

$$\gcd(\gcd(a,b),y)=\gcd(d_1,d_2).$$

(c) Suppose that $\gcd(b,a)=1$. Prove that $\gcd(b+a,b-a)\leq 2$.

Solution:

(a) Since $c|(a\cdot b)$, we know that $kc=ab$ for some integer k. By Euclidean algorithm, we also know that $\gcd(b,c)=sb+tc$ for some integers s and

t. Thus, we have

$$\begin{aligned} a \cdot \gcd(b,c) &= a \cdot (sb + tc) \\ &= asb + atc \\ &= skc + atc \\ &= (sk + at) \cdot c. \end{aligned}$$

Therefore, we have $c | (a \cdot \gcd(b,c))$.

(b) To begin with, we show that $\gcd(\gcd(a,b), y) \leq \gcd(d_1, d_2)$. Suppose that $d | \gcd(a,b)$ and $d|y$. Since $d | \gcd(a,b)$, we know that $d|a$ and $d|b$ by the definition of gcd. Thus, it follows from $d|a$ and $d|y$ that $d | \gcd(a,y) = d_1$. Similarly, $d|b$ and $d|y$ so $d | \gcd(b,y) = d_2$. By $d|d_1$ and $d|d_2$, we know that $d | \gcd(d_1, d_2)$. Hence, $d \leq \gcd(d_1, d_2)$.

Next we show $\gcd(d_1, d_2) \leq \gcd(\gcd(a,b), y)$. Suppose that $d|d_1$ and $d|d_2$. As $d | \gcd(a,y) = d_1$, we know $d|a$ and $d|y$. Similarly, as $d | \gcd(b,y) = d_2$ we know $d|b$ and $d|y$. Thus, $d|a$, $d|b$ and $d|y$. Because $d|a$ and $d|b$ we know $d | \gcd(a,b)$. Then $d | \gcd(a,b)$ and $d|y$, we know $\gcd(d_1, d_2) \leq \gcd(\gcd(a,b), y)$.

(c) 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

(a) State Fermat's little theorem.

(b) Show that Fermat's little theorem does not hold if p is not prime.

(c) Computer $302^{302} \pmod{11}$.

Solution:

(a) If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

(b) Take $p = 4$ and $a = 6$. Note that 6 is not divisible by 4 and that

$$\begin{aligned} 6^{4-1} \bmod 4 &\equiv (3 \cdot 2)^3 \pmod 4 \\ &\equiv 2^3 \cdot 3^3 \pmod 4 \\ &\equiv 8 \cdot 3^3 \pmod 4 \\ &\equiv 0. \end{aligned}$$

(c) By Fermat's little theorem, we have

$$\begin{aligned} 302^{302} \pmod{11} &\equiv (27 \cdot 11 + 5)^{302} \pmod{11} \\ &\equiv 5^{302} \pmod{11} \\ &\equiv 5^{30 \cdot 10 + 2} \pmod{11} \\ &\equiv 5^2 \cdot (5^{10})^{30} \pmod{11} \\ &\equiv 5^2 \pmod{11} \\ &\equiv 3. \end{aligned}$$

□

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.

$\square$

Q.6 Prove that if a and m are positive integer such that $\gcd(a, m) = 1$ then the function

$$f : \{0, \ldots, m-1\} \rightarrow \{0, \ldots, m-1\}$$

defined by

$$f(x) = (a \cdot x) \bmod m$$

is a bijection.

Solution:

Since $\gcd(a, m) = 1$ we know that a has an inverse modulo m. Let b be such an inverse, i.e.,

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

To show that f is a bijection, we need to show that it is one-to-one and onto. Let $S = \{0, \ldots, m-1\}$ denote the domain and codomain. We first show that f is one-to-one. Assume that $x, y \in S$ and $f(x) = f(y)$, i.e.,

$$ax \bmod m = ay \bmod m.$$

This is equivalent to saying that

$$ax \equiv ay \pmod{m}.$$

Multiplying both sides by b, we have

$$bax \equiv bay \pmod{m},$$

which is just

$$x \equiv y \pmod{m}.$$

Thus, $m | x - y$. Note that since $0 \leq x, y < m$, we have $|x - y| < m$. Thus, this is only possible if $x = y = 0$ or $x = y$ as desired.

To show that f is onto, let $z \in S$ be some element in the codomain. Let

$$x = bz \bmod m,$$

and note that $x \in S$ and

$$ax \equiv abz \equiv z \pmod{m}.$$

Since $z \in \{0, \ldots, m-1\}$, this means that $ax \bmod m = z$. Thus, $f(x) = z$, as desired.

$\square$

Q.7 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.

$\square$

Q.8 Convert the decimal expansion of each of these integers to a binary expansion.
(a) 231 (b) 4532 (c) 97644
Solution: (a) 11100111
(b) 1000110110100
(c) 10111110101101100

$\square$

Q.9 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

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

$\square$

Q.10 Compute the following without calculator. You may find Fermat's little theorem useful for some of these.

(1) The last decimal digit of 3^{1000}

(2) $3^{1000} \bmod 31$

(3) $3/16$ in $\mathbb{Z}_{31}$

Solution:

(1) The last decimal digit of 3^{1000} is equivalent to computing $3^{1000} \bmod 10$. By Fermat's little theorem, we have $3^4 \equiv 1 \pmod 5$. Thus, $3^{1000} \equiv 1 \pmod 2$ and $3^{1000} \equiv 3^{4\times 250} \equiv 1 \pmod 5$. Then by Chinese remainder theorem, we have $3^{1000} \bmod 10 = 1$.

(2) By Fermat's little theorem, we have $3^{30} \equiv 1 \pmod{31}$. Then we have

$$3^{1000} \bmod 31 = 3^{30*33+10} \bmod 31 = 3^{10} \bmod 31.$$

By $3^2 \bmod 31 = 9$, $3^4 \bmod 31 = 9*9 \bmod 31 = 19$, $3^8 \bmod 31 = 19*19 \bmod 31 = 20$, we have $3^10 \bmod 31 = 9*20 \bmod 31 = 25$.

(3) In $\mathbb{Z}_{31}$, we have $3/16 = 3*16^{-1} \pmod{31}$. Since $\gcd(16, 31) = 1$, by extended Euclidean algorithm, we have $1 = 2\times 16 - 31$. Thus, the modular inverse of 16 in $\mathbb{Z}_{31}$ is 2. Then we have $3/16 = 3*2 = 6$.

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 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.13 Show that if a, b, and m are integers such that $m \geq 2$ and $a \equiv b \bmod m$, then $\gcd(a, m) = \gcd(b, m)$.
Solution:

From $a \equiv b \bmod m$, we know that $b = a + sm$ for some integer s. Now if d is a common divisor of a and m, then it divides the right-hand side of this equation, so it also divides b. We can rewrite the equation as $a = b - sm$, and then by similar reasoning, we see that every common divisor of b and m is also a divisor of a. This shows that the set of common divisors of a and m is equal to the set of common divisors of b and m, so certainly $\gcd(a, m) = \gcd(b, m)$.

$\square$

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 $q_1, q_2, \ldots, q_n$, 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 $q_1, q_2, \ldots, q_n$, 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 $q_1, q_2, \ldots, q_n$, 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 $3^{302} \bmod 5$, $3^{302} \bmod 7$, and $3^{302} \bmod 11$.

(b) Use your results from part (c) and the Chinese remainder theorem to find $3^{302} \bmod 385$. (Note that $385 = 5 \cdot 7 \cdot 11$.)

Solution:

(a) By Fermat's little theorem we know that $3^4 \equiv 1 \pmod 5$; therefore $3^{300} = (3^4)^{75} \equiv 1^{75} \equiv 1 \pmod 5$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \cdot 1 = 9 \pmod 5$, so $3^{302} \bmod 5 = 4$. Similarly, $3^6 \equiv 1 \bmod 7$; therefore $3^{300} = (3^6)^{50} \equiv 1 \pmod 5$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \pmod 7$, so $3^{302} \bmod 7 = 2$. Finally, $3^{10} \equiv 1 \pmod{11}$; therefore $3^{300} = (3^{10})^{30} \equiv 1 \pmod{11}$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \pmod{11}$, so $3^{302} \bmod 11 = 9$.

(b) Since 3^{302} is congruent to 9 modulo 5, 7, and 11, it is also congruent to 9 modulo 385. (This is a particularly trivial application of the Chinese remainder theorem.)

$\square$

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 $a \equiv b \pmod{m_1 m_2 \cdots m_n}$.

$\square$

Q.18 For a collection of balls, the number is not known. If we count them by 2's, we have 1 left over; by 3's, we have nothing left; by 4, we have 1 left over; by 5, we have 4 left over; by 6, we have 3 left over; by 7, we have nothing left; by 8, we have 1 left over; by 9, nothing is left. How many balls are there? Give the details of your calculation.

Solution: This is equivalent to solve the following system of congruences:

$$x \equiv 1 \pmod 2$$
$$x \equiv 0 \pmod 3$$
$$x \equiv 1 \pmod 4$$
$$x \equiv 4 \pmod 5$$
$$x \equiv 3 \pmod 6$$
$$x \equiv 0 \pmod 7$$
$$x \equiv 1 \pmod 8$$
$$x \equiv 0 \pmod 9.$$

Since $x \equiv 3 \pmod 6$, we have $x = 6k + 3$ and further have $x \equiv 1 \pmod 2$ and $x \equiv 0 \pmod 3$. Thus, $x \equiv 3 \pmod 6$ is redundant in the system and can be ignored. Note that $x \equiv 1 \pmod 8$ implies both $x \equiv 1 \pmod 2$ and $x \equiv 1 \pmod 4$, and $x \equiv 0 \pmod 9$ implies $x \equiv 0 \pmod 3$. We thus have an equivalent but refreshed system of congruences as:

$$x \equiv 4 \pmod 5$$
$$x \equiv 0 \pmod 7$$
$$x \equiv 1 \pmod 8$$
$$x \equiv 0 \pmod 9.$$

All the m_i's are pairwise relatively prime, and we are able to use Chinese Remainder Theorem or back substitution to solve this system of congruences. Note that $m = 5 \cdot 7 \cdot 8 \cdot 9 = 2520$, $M_1 = 7 \cdot 8 \cdot 9 = 504$, $M_2 = 5 \cdot 8 \cdot 9 = 360$, $M_3 = 5 \cdot 7 \cdot 9 = 315$, and $M_4 = 5 \cdot 7 \cdot 8 = 280$. By extended Euclidean algorithm, we have $y_1 = 4$, $y_2 = 5$, $y_3 = 3$ and $y_4 = 1$. Then by Chinese Remainder Theorem, we have the solution is

$$x \equiv 4 * 504 * 4 + 0 + 1 * 315 * 3 + 0 \pmod{2520} \equiv 1449 \pmod{2520}.$$

□

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

$\square$

Q.20 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.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. Prove that for all integers $n \geq 3$, $\phi(n)$ is even.

Solution: If n is odd, for every integer a with $\gcd(a, n) = 1$, we also have $\gcd(n-a, n) = \gcd(a, n) = 1$ and $n - a \neq a$ for n odd. Thus, $\phi(n)$ must be even for n odd.

For n even, we discuss two cases. If $n = 4k+2$ for an integer k, then we have

$$\phi(n) = \phi(4k+2) = \phi(2)\phi(2k+1) = \phi(2k+1),$$

which is again odd, and thus is even. If $n = 4k$ for an integer k, then we have

$$\phi(n) = \phi(4k) = \phi(4 \cdot 2^r k') = \phi(2^{r+2}k') = \phi(2^{r+2})\phi(k') = 2^{r+1}\phi(k'),$$

where k' is odd. Thus, $\phi(n)$ is also even for $n = 4k$.

$\square$

Q.22 Recall the RSA public key cryptosystem: Bob posts a public key (n, e) and keeps a secret key d. When Alice wants to send a message $0 < M < n$ to Bob, she calculates $C = M^e \pmod{n}$ and sends C to Bob. Bob then decrypts this by calculating $C^d \pmod{n}$. In class we learnt that in order to make this scheme work, n, e, d must have special properties.

For each of the three public/secret key pairs listed below, answer whether it is a **valid** set of RSA public/secret key pairs (whether the pair satisfies the required properties), and explain your answer.

(a) $(n, e) = (91, 25)$, $d = 51$

(b) $(n, e) = (91, 25)$, $d = 49$

(c) $(n, e) = (84, 25)$, $d = 37$

Solution:
Recall that the conditions for a pair to be correct is

(i) $n = pq$ where p and q are prime numbers

(ii) $ed \equiv 1 \pmod{\phi(n)}$, where $\phi(n) = (p-1)(q-1)$.

(a) $(n, e) = (91, 25)$, $d = 51$

This is not a valid key pair. It is true that $n = 7 \cdot 13$, so p, q are prime. But $\phi(n) = 72$, and $25 \cdot 51 \not\equiv 1 \pmod{72}$.

(b) $(n, e) = (91, 25)$, $d = 49$

This is a valid key pair since $n = 7 \cdot 13$, and $25 \cdot 49 \equiv 1 \pmod{72}$.

(c) This is not a valid key pair since $n = 7 \cdot 12$ and 12 is not a prime.

$\square$

Q. 23 Consider the RSA system. Let (e, d) be a key pair for the RSA. Define

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

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

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

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

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 $C^{d'} \bmod n = M$.

Case `II`: $\gcd(M, n) = p$. $M = tp$ 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.

$\square$