CS215: Discrete Math (H)
2024 Fall Semester Written Assignment # 3
Due: Nov. 13th, 2024, please submit at the beginning of class

Q.1 What are the prime factorizations of

(a) 8085

(b) 10!

Solution:

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

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

$\square$

Q.2

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

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

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

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

$\square$

Q.3 For three integers a, b, y, suppose that $\gcd(a, y) = d_1$ and $\gcd(b, y) = d_2$. Prove that

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

Solution: To begin, we show $\gcd(\gcd(a, b), y) \leq \gcd(d_1, d_2)$. Suppose that $d | \gcd(a, b)$ and $d|y$. As $d | \gcd(a, b)$ we know $d|a$ and $d|b$. Thus, $d|a$ and $d|y$ so $d | \gcd(a, y) = d_1$. Similarly, $d|b$ and $d|y$ so $d | \gcd(b, y) = d_2$. Because $d|d_1$ and $d|d_2$ we know $d | \gcd(d_1, d_2)$. Hence we have $d \leq \gcd(d_1, d_2)$.

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 show $d | \gcd(a, b)$. Then $d | \gcd(a, b)$ and $d|y$. We know $d | \gcd(\gcd(a, b), y)$. The theorem follows.

[Alternate solution.] We can also prove this via unique prime factorizations. Let $p_1, p_2, \ldots, p_k$ be the first k primes for some large k, then for a, b and y, we can define sequences of integers (possibly zero) $a_1, \ldots, a_k$, $b_1, \ldots, b_k$

and $y_1, \ldots, y_k$ such that

$$a = \prod_{i=1}^{k} p_i^{a_i} = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \quad b = \prod_{i=1}^{k} p_i^{b_i} \quad \text{and } y = \prod_{i=1}^{k} p_i^{y_i}.$$

Now we have

$$\gcd(a,b) = \prod_{i=1}^{k} p_i^{\min\{a_i,b_i\}} \quad \text{and } \gcd(a,b) = \prod_{i=1}^{k} p_i^{\min\{\min\{a_i,b_i\},y\}}.$$

Similarly,

$$d_1 = \gcd(a,y) = \prod_{i=1}^{k} p_i^{\min\{a_i,y_i\}} \quad \text{and } d_2 = \gcd(b,y) = \prod_{i=1}^{k} p_i^{\min\{b_i,y_i\}}$$

so

$$\gcd(d_1,d_2) = \prod_{i=1}^{k} p_i^{\min\{\min\{a_i,y_i\},\min\{b_i,y_i\}\}}.$$

But, since $\min\{\min\{a_i,b_i\},y_i\} = \min\{\min\{a_i,y_i\},\min\{b_i,y_i\}\}$, these values are equal.

$\square$

Q.4 Prove the following statement. If $c|(a \cdot b)$, then $c|(a \cdot \gcd(b,c))$.
Solution: 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 $c|(a \cdot \gcd(b,c))$.

$\square$

Q.5 Solve the following modular equation.

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

Solution: Applying Euclidean algorithm, we have

$$\begin{aligned}
312 &= 3 \cdot 97 + 21 \\
97 &= 4 \cdot 21 + 13 \\
21 &= 1 \cdot 13 + 8 \\
13 &= 1 \cdot 8 + 5 \\
8 &= 1 \cdot 5 + 3 \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1.
\end{aligned}$$

Reading Euclidean algorithm backwards we have $1 = 37 \cdot 312 - 119 \cdot 97$. So, $312 \cdot 37 \equiv 1 \pmod{97}$. Thus, $x \equiv 37 \cdot 3 \equiv 111 \equiv 14 \pmod{97}$.

□

Q.6 Find counterexamples to each of these statements about congruences.

(a) If $ac \equiv bc \pmod{m}$, where a, b, c, and m are integers with $m \geq 2$, then $a \equiv b \pmod{m}$.

(b) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where a, b, c, d, and m are integers with c and d positive and $m \geq 2$, then $a^c \equiv b^d \pmod{m}$.

Solution:

(a) Let $m = c = 2$, $a = 0$ and $b = 1$. Then $0 = ac \equiv bc = 2 \pmod{2}$, but $0 = a \not\equiv b = 1 \pmod{2}$.

(b) Let $m = 5$, $a = b = 3$, $c = 1$, and $d = 6$. Then $3 \equiv 3 \pmod{5}$ and $1 \equiv 6 \pmod{5}$, but $3^1 = 3 \not\equiv 4 \equiv 729 = 3^6 \pmod{5}$.

□

Q.7 Prove that if a and m are positive integer such that $\gcd(a, m) = 1$ then the function

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

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.

□

Q.8 Convert the decimal expansion of each of these integers to a binary expansion.

(a) 231 (b) 4532

Solution: (a) 11100111

(b) 1000110110100

□

Q.9 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.10 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.11 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.12

(1) Show that if n is an integer then $n^2 \equiv 0$ or $1 \pmod{4}$.

(2) Show that if m is a positive integer of the form $4k+3$ for some nonnegative integer k, then m is not the sum of the squares of two integers.

Solution:

(1) There are two cases. If n is even, then $n = 2k$ for some integer k, so $n^2 = 4k^2$, which means that $n^2 \equiv 0 \pmod 4$. If n is odd, then $n = 2k+1$ for some integer k, so $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, which means that $n^2 \equiv 1 \pmod 4$.

(2) By (1), the sum of two squares must be either $0+0=0$, $0+1=1$, or $1+1=2$, modulo 4, never 3, and therefore not of the form $4k+3$.

$\square$

Q.13

(a) State Fermat's little theorem.

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

(c) Compute $302^{302} \pmod{11}$, $4762^{5367} \pmod{13}$, $2^{39674} \pmod{523}$.

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

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

Note that 13 is a prime. Then by Fermat's little theorem, we have

$$\begin{aligned} 4762^{5367} \pmod{13} &\equiv (366 \cdot 13 + 4)^{5367} \pmod{13} \\ &\equiv 4^{5367} \pmod{13} \\ &\equiv 4^{447 \cdot 12 + 3} \pmod{13} \\ &\equiv 4^{3} \pmod{13} \\ &\equiv 64 \pmod{13} \\ &\equiv 12. \end{aligned}$$

Note that 523 is a prime. Then by Fermat's little theorem, we have

$$\begin{aligned} 2^{39674} \pmod{523} &\equiv 2^{76 \cdot 522 + 2} \pmod{523} \\ &\equiv 2^{2} \pmod{523} \\ &\equiv 4. \end{aligned}$$

□

Q.14 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.15 Solve the system of congruence $x \equiv 3 \pmod 6$ and $x \equiv 4 \pmod 7$ using the methods of Chinese Remainder Theorem or back substitution.

Solution:

By definition, the first congruence can be written as $x = 6t + 3$ where t is an integer. Substituting this expression for x into the second congruence tells us that $6t + 3 \equiv 4 \pmod 7$, which can be easily be solved to show that

$t \equiv 6 \pmod 7$. From this we can write $t = 7u + 6$ for some integer u. Thus, $x = 6t + 3 = 6 \cdot (7u + 6) + 3 = 42u + 39$. Thus, our answer is all numbers congruent to 39 modulo 42.

$\square$

Q.16 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:

$$
\begin{aligned}
x &\equiv 1 \pmod 2 \\
x &\equiv 0 \pmod 3 \\
x &\equiv 1 \pmod 4 \\
x &\equiv 4 \pmod 5 \\
x &\equiv 3 \pmod 6 \\
x &\equiv 0 \pmod 7 \\
x &\equiv 1 \pmod 8 \\
x &\equiv 0 \pmod 9.
\end{aligned}
$$

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:

$$
\begin{aligned}
x &\equiv 4 \pmod 5 \\
x &\equiv 0 \pmod 7 \\
x &\equiv 1 \pmod 8 \\
x &\equiv 0 \pmod 9.
\end{aligned}
$$

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.17 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.18 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.19 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.

□

Q.20 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: <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

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

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

□