1 Modular Practice

Solve the following modular arithmetic equations for $x$ and $y$.

(a) $9x + 5 \equiv 7 \pmod{11}$.
(b) Show that $3x + 15 \equiv 4 \pmod{21}$ does not have a solution.
(c) The system of simultaneous equations $3x + 2y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.
(d) $13^{2019} \equiv x \pmod{12}$.
(e) $7^{21} \equiv x \pmod{11}$.

Solution:

(a) Subtract 5 from both sides to get:

$$9x \equiv 2 \pmod{11}.$$ 

Now since $\gcd(9, 11) = 1$, 9 has a (unique) inverse mod 11, and since $9 \times 5 = 45 \equiv 1 \pmod{11}$ the inverse is 5. So multiply both sides by $9^{-1} \equiv 5 \pmod{11}$ to get:

$$x \equiv 10 \pmod{11}.$$ 

(b) Notice that any number $y \equiv 4 \pmod{21}$ can be written as $y = 4 + 21k$ (for some integer $k$). Evaluating $y \pmod{3}$, we get $y \equiv 1 \pmod{3}$. Since the right side of the equation is 1 (mod 3), the left side must be as well. However, $3x + 15$ will never be 1 (mod 3) for any value of $x$. Thus, there is no possible solution.

(c) First, subtract the first equation from double the second equation to get:

$$2(2x + y) - (3x + 2y) \equiv x \equiv 1 \pmod{7}.$$ 

Now plug into the second equation.

$$2 + y \equiv 4 \pmod{7},$$

so the system has the solution $x \equiv 1 \pmod{7}$, $y \equiv 2 \pmod{7}$. 

(d) We use the fact that
\[ 13 \equiv 1 \pmod{12} \]
Thus, we can rewrite the equation as
\[ x \equiv 13^{2019} \equiv 1^{2019} \equiv 1 \pmod{12}. \]

(e) One way to solve exponentiation problems is to test values until one identifies a pattern.

\[
\begin{align*}
7^1 &\equiv 7 \pmod{11} \\
7^2 &\equiv 49 \equiv 5 \pmod{11} \\
7^3 &= 7 \cdot 7^2 \equiv 7 \cdot 5 \equiv 2 \pmod{11} \\
7^4 &= 7 \cdot 7^3 \equiv 7 \cdot 2 \equiv 3 \pmod{11} \\
7^5 &= 7 \cdot 7^4 \equiv 7 \cdot 3 \equiv 10 \equiv -1 \pmod{11}.
\end{align*}
\]

We theoretically could continue this until we the sequence starts repeating. However, notice that if \( 7^5 \equiv -1 \implies 7^{10} = (7^5)^2 \equiv (-1)^2 \equiv 1 \pmod{11} \).

Similarly, \( 7^{20} = (7^{10})^2 \equiv 1^2 \equiv 1 \pmod{11} \). As a final step, we have \( 7^{21} = 7 \cdot 7^{20} \equiv 7 \cdot 1 = 7 \pmod{11} \).

2 Nontrivial Modular Solutions

(a) What are all the possible perfect cubes modulo 7?

(b) Show that any solution to \( a^3 + 2b^3 \equiv 0 \pmod{7} \) must satisfy \( a \equiv b \equiv 0 \pmod{7} \).

(c) Using part (b), prove that \( a^3 + 2b^3 = 7a^2b \) has no non-trivial solutions \((a, b)\) in the integers. In other words, there are no integers \(a\) and \(b\), that satisfy this equation, except the trivial solution \(a = b = 0\).

[\text{Hint: Consider some nontrivial solution } (a, b) \text{ with the smallest value for } |a| \text{ (why are we allowed to consider this?)}. \text{ Then arrive at a contradiction by finding another solution } (a', b') \text{ with } |a'| < |a|.]\]

Solution:

(a) Checking by hand, the only perfect cubes modulo 7 are 0, 1, and 6 \( \equiv -1 \):
\[
\begin{align*}
0^3 &\equiv 0 \pmod{7} & 4^3 &\equiv 1 \pmod{7} \\
1^3 &\equiv 1 \pmod{7} & 5^3 &\equiv -1 \pmod{7} \\
2^3 &\equiv 1 \pmod{7} & 6^3 &\equiv -1 \pmod{7} \\
3^3 &\equiv -1 \pmod{7} &
\end{align*}
\]

(b) Considering the equation \( a^3 + 2b^3 \equiv 0 \pmod{7} \) and considering all cases for \( a^3 \) and \( b^3 \), the only way that \( a^3 + 2b^3 \equiv 0 \pmod{7} \) is if \( a^3 \equiv b^3 \equiv 0 \pmod{7} \). Thus \( a \equiv b \equiv 0 \pmod{7} \).
(c) We first show that if \((a, b)\) is a solution to \(a^3 + 2b^3 = 7a^2b\), then \(a = 0\) implies that \(b = 0\). In other words, if \(a = 0\), then the solution must be trivial. To see why this is the case, suppose that \(a = 0\). Then \(b^3 = 0\), and so \(b = 0\). Thus, any nontrivial solution must have \(a \neq 0\), or equivalently, \(|a| > 0\).

If \((a, b)\) is a solution to the original equation, then this is also a solution to
\[
a^3 + 2b^3 \equiv 0 \pmod{7}.
\]

From Part (b), we know that \(a, b\) are all divisible by 7, which in turn means that \(a^3, b^3\) are divisible by \(7^3\). Thus, we can divide the entire original equation by \(7^3\), to see that
\[
\left(\frac{a}{7}\right)^3 + 2\left(\frac{b}{7}\right)^3 = 7\left(\frac{a}{7}\right)^2 \left(\frac{b}{7}\right).
\]

Indeed, \((a/7, b/7)\) is another solution where all the values are integers, and \(|a/7| < |a|\) (as \(|a| > 0\)). We’ve reached a contradiction to our initial assumption, which was that \((a, b)\) was the solution with the least value of \(|a|\). (This is a valid assumption since the \(|a|\) are positive integers, and a non-empty set of positive integers has a minimum.) Thus, there does not exist a nontrivial solution to \(a^3 + 2b^3 = 7a^2b\).

3 Wilson’s Theorem

Wilson’s Theorem states the following is true if and only if \(p\) is prime:
\[
(p - 1)! \equiv -1 \pmod{p}.
\]

Prove both directions (it holds if AND only if \(p\) is prime).

Hint for the if direction: Consider rearranging the terms in \((p - 1)! = 1 \cdot 2 \cdot \ldots \cdot (p - 1)\) to pair up terms with their inverses, when possible. What terms are left unpaired?

Hint for the only if direction: If \(p\) is composite, then it has some prime factor \(q\). What can we say about \((p - 1)! \pmod{q}\)?

Solution:

Direction 1: If \(p\) is prime, then the statement holds.

For the integers \(1, \ldots, p - 1\), every number has an inverse. However, it is not possible to pair a number off with its inverse when it is its own inverse. This happens when \(x^2 \equiv 1 \pmod{p}\), or when \(p \mid x^2 - 1 = (x - 1)(x + 1)\). Thus, \(p \mid x - 1\) or \(p \mid x + 1\), so \(x \equiv 1 \pmod{p}\) or \(x \equiv -1 \pmod{p}\). Thus, the only integers from 1 to \(p - 1\) inclusive whose inverse is the same as itself are 1 and \(p - 1\).

We reconsider the product \((p - 1)! = 1 \cdot 2 \cdots p - 1\). The product consists of 1, \(p - 1\), and pairs of numbers with their inverse, of which there are \(p - 1 - 2 = \frac{p - 3}{2}\). The product of the pairs is 1 (since the product of a number with its inverse is 1), so the product \((p - 1)! \equiv 1 \cdot (p - 1) \cdot 1 \equiv -1 \pmod{p}\), as desired.
Direction 2: The expression holds only if \( p \) is prime (contrapositive: if \( p \) isn’t prime, then it doesn’t hold).

We will prove by contradiction that if some number \( p \) is composite, then \( (p - 1)! \not\equiv -1 \pmod{p} \); Hypothetically assume that \( (p - 1)! \equiv -1 \pmod{p} \). Note that this means we can write \( (p - 1)! \) as \( p \cdot k - 1 \) for some integer \( k \).

Since \( p \) isn’t prime, it has some prime factor \( q \) where \( 2 \leq q \leq n - 2 \), and we can write \( p = q \cdot r \).

Plug this into the expression for \( (p - 1)! \) above, yielding us \( (p - 1)! = (q \cdot r)k - 1 = q(rk) - 1 \implies (p - 1)! \equiv -1 \pmod{q} \). However, we know \( q \) is a term in \( (p - 1)! \), so \( (p - 1)! \equiv 0 \pmod{q} \). Since \( 0 \not\equiv 1 \pmod{q} \), we have reached our contradiction.

## 4 Ferma’t’s Little Theorem

Without using induction, prove that \( \forall n \in \mathbb{N}, n^7 - n \) is divisible by 42.

**Solution:**

Let \( n \in \mathbb{N} \). We begin by breaking down 42 into prime factors: 42 = 7 \times 3 \times 2. Since 7, 3, and 2 are prime, we can apply Ferma’t’s Little Theorem, which says that \( a^p \equiv a \pmod{p} \), to get the congruences

\[
\begin{align*}
n^7 &\equiv n \pmod{7}, \\
n^3 &\equiv n \pmod{3}, \quad \text{and} \\
n^2 &\equiv n \pmod{2}.
\end{align*}
\]

Now, let’s take (3) and multiply it by \( n^3 \cdot n \). This gives us

\[
n^7 \equiv n^3 \cdot n \equiv n \cdot n \cdot n \equiv n^3 \pmod{3},
\]

and since by (3), \( n^3 \equiv n \pmod{3} \), this gives

\[
n^7 \equiv n \pmod{3}.
\]

Similarly, we take (4) and multiply by \( n^2 \cdot n^2 \cdot n \) to get

\[
n^7 \equiv n^2 \cdot n^2 \cdot n \equiv n^4 \pmod{2}.
\]

Notice that \( n^4 \equiv n^2 \cdot n^2 \equiv n \cdot n \equiv n^2 \pmod{2} \), and by (4) \( n^2 \equiv n \pmod{2} \), so we have

\[
n^7 \equiv n \pmod{2}.
\]

Thus,

\[
\begin{align*}
n^7 &\equiv n \pmod{7}, \\
n^7 &\equiv n \pmod{3}, \quad \text{and} \\
n^7 &\equiv n \pmod{2}.
\end{align*}
\]
Let \( x = n^7 - n \). By the Chinese Remainder Theorem, the system of congruences

\[
\begin{align*}
    x &\equiv 0 \pmod{7} \\
    x &\equiv 0 \pmod{3} \\
    x &\equiv 0 \pmod{2}
\end{align*}
\]

has a unique solution modulo \( 2 \cdot 3 \cdot 7 = 42 \), and this unique solution is \( x \equiv 0 \pmod{42} \). So, we have that \( n^7 - n \equiv 0 \pmod{42} \), which means \( n^7 - n \) is divisible by 42.

5. **Euler’s Totient Function**

Euler’s totient function is defined as follows:

\[
\phi(n) = |\{i : 1 \leq i \leq n, \gcd(n, i) = 1\}|
\]

In other words, \( \phi(n) \) is the total number of positive integers less than or equal to \( n \) which are relatively prime to it. We develop a general formula to compute \( \phi(n) \).

(a) Let \( p \) be a prime number. What is \( \phi(p) \)?

(b) Let \( p \) be a prime number and \( k \) be some positive integer. What is \( \phi(p^k) \)?

(c) Show that if \( \gcd(m, n) = 1 \), then \( \phi(mn) = \phi(m)\phi(n) \). (Hint: Use the Chinese Remainder Theorem.)

(d) Argue that if the prime factorization of \( n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \), then

\[
\phi(n) = n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}.
\]

**Solution:**

(a) Since \( p \) is prime, all the numbers from 1 to \( p - 1 \) are relatively prime to \( p \).

So, \( \phi(p) = p - 1 \).

(b) The only positive integers less than \( p^k \) which are not relatively prime to \( p^k \) are multiples of \( p \).

Why is this true? This is so because the only possible prime factor which can be shared with \( p^k \) is \( p \). Hence, if any number is not relatively prime to \( p^k \), it has to have a prime factor of \( p \) which means that it is a multiple of \( p \).

The multiples of \( p \) which are \( \leq p^k \) are \( 1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p \). There are \( p^{k-1} \) of these.

The total number of positive integers less than or equal to \( p^k \) is \( p^k \).

So \( \phi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p - 1) \).
(c) Let $M$ be the set of positive integers $1 \leq i \leq m$ such that $\gcd(i, m) = 1$, and let $N$ be the set of positive integers $1 \leq j \leq m$ such that $\gcd(j, n) = 1$. Since $\gcd(m, n) = 1$, the Chinese Remainder Theorem gives that every choice $(i, j) \in M \times N$ corresponds bijectively with an integer $1 \leq k \leq mn$, where $k \equiv i \pmod{m}$ and $k \equiv j \pmod{n}$. Thus, $\gcd(k, mn) = 1$, so the Chinese Remainder Theorem associates each $(i, j)$ to a unique $1 \leq k \leq mn$ relatively prime to $mn$.

Moreover, note that each $1 \leq k \leq mn$ relative prime to $mn$ can be associated with an $(i, j) \in M \times N$ such that $k \equiv i \pmod{m}$ and $k \equiv j \pmod{n}$. Thus, we have a bijection between $M \times N$ and the set of positive integers $1 \leq k \leq mn$ relatively prime to $mn$.

Since $|M| = \phi(m)$, $|N| = \phi(n)$, and the set of positive integers $1 \leq k \leq mn$ relatively prime to $mn$ has cardinality $\phi(mn)$ (by definition), we conclude that $\phi(m)\phi(n) = \phi(mn)$.

(d) Applying part (c) inductively, we conclude that

$$
\phi(n) = \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \frac{n \prod_{i=1}^{k} p_i - 1}{p_i}
$$

6 Euler’s Totient Theorem

Euler’s Totient Theorem states that, if $n$ and $a$ are coprime,

$$
a^{\phi(n)} \equiv 1 \pmod{n}
$$

where $\phi(n)$ (known as Euler’s Totient Function) is the number of positive integers less than or equal to $n$ which are coprime to $n$ (including 1).

(a) Let the numbers less than $n$ which are coprime to $n$ be $m_1, m_2, \ldots, m_{\phi(n)}$. Argue that the set

$$\{am_1, am_2, \ldots, am_{\phi(n)}\}
$$

is a permutation of the set

$$\{m_1, m_2, \ldots, m_{\phi(n)}\}.
$$

In other words, prove that

$$f : \{m_1, m_2, \ldots, m_{\phi(n)}\} \to \{m_1, m_2, \ldots, m_{\phi(n)}\},
$$

is a bijection, where $f(x) := ax \pmod{n}$. 

CS 70, Fall 2022, HW 04
(b) Prove Euler’s Theorem. (Hint: Recall the FLT proof.)

Solution:

(a) This problem mirrors the proof of Fermat’s Little Theorem, except now we work with the set \( \{m_1, m_2, \ldots, m_{\phi(n)}\} \).

Since \( m_i \) and \( a \) are both coprime to \( n \), so is \( a \cdot m_i \). Suppose \( a \cdot m_i \) shared a common factor with \( n \), and WLOG, assume that it is a prime \( p \). Then, either \( p \mid a \) or \( p \mid m_i \). In either case, \( p \) is a common factor between \( n \) and one of \( a \) or \( m_i \), contradiction.

We now prove that \( f \) is injective. Suppose we have \( f(x) = f(y) \), so \( ax \equiv ay \pmod{n} \). Since \( a \) has a multiplicative inverse \( \pmod{n} \), we see \( x \equiv y \pmod{n} \), thus showing that \( f \) is injective.

We continue to show that \( f \) is surjective. Take any \( y \) that is relatively prime to \( n \). Then, we see that \( f(a^{-1}y) \equiv y \pmod{n} \), so therefore, there is an \( x \) such that \( f(x) = y \). Furthermore, \( a^{-1}y \pmod{n} \) is relatively prime to \( n \), since we are multiplying two numbers that are relatively prime to \( n \).

(b) Since both sets have the same elements, just in different orders, multiplying them together gives

\[
m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)} \equiv a m_1 \cdot a m_2 \cdot \ldots \cdot a m_{\phi(n)} \pmod{n}
\]

and factoring out the \( a \) terms,

\[
m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)} \equiv a^{\phi(n)} (m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)}) \pmod{n}.
\]

Thus we have \( a^{\phi(n)} \equiv 1 \pmod{n} \).

7 Sparsity of Primes

A prime power is a number that can be written as \( p^i \) for some prime \( p \) and some positive integer \( i \). So, \( 9 = 3^2 \) is a prime power, and so is \( 8 = 2^3 \). \( 42 = 2 \cdot 3 \cdot 7 \) is not a prime power.

Prove that for any positive integer \( k \), there exists \( k \) consecutive positive integers such that none of them are prime powers.

Hint: This is a Chinese Remainder Theorem problem. We want to find \( x \) such that \( x + 1, x + 2, \ldots, x + k \) are all not powers of primes. We can enforce this by saying that \( x + 1 \) through \( x + k \) each must have two distinct prime divisors.

Solution:

We want to find \( x \) such that \( x + 1, x + 2, x + 3, \ldots, x + k \) are all not powers of primes. We can enforce this by saying that \( x + 1 \) through \( x + k \) each must have two distinct prime divisors. So, select \( 2k \).
primes, \( p_1, p_2, \ldots, p_{2k} \), and enforce the constraints

\[
\begin{align*}
x + 1 & \equiv 0 \pmod{p_1 p_2} \\
x + 2 & \equiv 0 \pmod{p_3 p_4} \\
& \quad \vdots \\
x + i & \equiv 0 \pmod{p_{2i-1} p_{2i}} \\
& \quad \vdots \\
x + k & \equiv 0 \pmod{p_{2k-1} p_{2k}}.
\end{align*}
\]

By Chinese Remainder Theorem, we can calculate the value of \( x \), so this \( x \) must exist, and thus, \( x + 1 \) through \( x + k \) are not prime powers.

What’s even more interesting here is that we could select any 2\( k \) primes we want!