1 Baby Fermat

Assume that $a$ does have a multiplicative inverse mod $m$. Let us prove that its multiplicative inverse can be written as $a^k \mod m$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \ldots \mod m$. Prove that this sequence has repetitions. 
\textbf{(Hint:} Consider the Pigeonhole Principle.)

(b) Assuming that $a^i \equiv a^j \mod m$, where $i > j$, what can you say about $a^{i-j} \mod m$?

(c) Prove that the multiplicative inverse can be written as $a^k \mod m$. What is $k$ in terms of $i$ and $j$?

\textbf{Solution:}

(a) There are only $m$ possible values mod $m$, and so after the $m$-th term we should see repetitions.

The Pigeonhole principle applies here - we have $m$ boxes that represent the different unique values that $a^k$ can take on \mod m. Then, we can view $a, a^2, a^3, \ldots$ as the objects to put in the $m$ boxes. As soon as we have more than $m$ objects (in other words, we reach $a^{m+1}$ in our sequence), the Pigeonhole Principle implies that there will be a collision, or that at least two numbers in our sequence take on the same value \mod m.

(b) We will temporarily use the notation $a^*$ for the multiplicative inverse of $a$ to avoid confusion.

If we multiply both sides by $(a^*)^j$ in the third line below, we get

\[
\begin{align*}
a^j & \equiv a^j \mod m, \\
ad^j a^{\cdots} a^\cdots a & \equiv a^j a^{\cdots} a^\cdots a \\
& \quad \text{\footnotesize \textit{j times}} \quad \text{\footnotesize \textit{j times}} \\
& \equiv a^j a^{\cdots} a^\cdots a^* a^\cdots a^* a^* \\
& \quad \text{\footnotesize \textit{j times}} \quad \text{\footnotesize \textit{j times}} \quad \text{\footnotesize \textit{j times}} \quad \text{\footnotesize \textit{j times}} \\
& \equiv 1 \mod m, \\
d^{i-j} & \equiv 1 \mod m.
\end{align*}
\]

(c) We can rewrite $a^{i-j} \equiv 1 \mod m$ as $a^{i-j-1} a \equiv 1 \mod m$. Therefore $a^{i-j-1}$ is the multiplicative inverse of $a$ \mod m.
2 Euler’s Totient Function

Euler’s totient function is defined as follows:

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

In other words, \( \varphi(n) \) is the total number of positive integers less than or equal to \( n \) which are relatively prime to it. Here is a property of Euler’s totient function that you can use without proof:

For \( m, n \) such that \( \gcd(m, n) = 1 \), \( \varphi(mn) = \varphi(m) \cdot \varphi(n) \).

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

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

(c) Let \( p \) be a prime number and \( a \) be a positive integer smaller than \( p \). What is \( a^{\varphi(p)} \pmod{p} \)?

(Hint: use Fermat’s Little Theorem.)

(d) Let \( b \) be a positive integer whose prime factors are \( p_1, p_2, \ldots, p_k \). We can write \( b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \).

Show that for any \( a \) relatively prime to \( b \), the following holds:

\[ \forall i \in \{1, 2, \ldots, k\}, \quad a^{\varphi(b)} \equiv 1 \pmod{p_i} \]

Solution:

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

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

(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 \( \varphi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p - 1) \).

(c) From Fermat’s Little Theorem, and part (a),

\[ a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \pmod{p} \]

(d) From the property of the totient function and part (b):
\[
\phi(b) = \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \\
= \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k}) \\
= p_1^{\alpha_1-1}(p_1-1) \cdot p_2^{\alpha_2-1}(p_2-1) \cdots p_k^{\alpha_k-1}(p_k-1)
\]

This shows that, for every \(p_i\), which is a prime factor of \(b\), we can write \(\phi(b) = c \cdot (p_i - 1)\), where \(c\) is some constant. Since \(a\) and \(b\) are relatively prime, \(a\) is also relatively prime with \(p_i\).

From Fermat’s Little Theorem:
\[
a^{\phi(b)} \equiv a^c(p_i-1) \equiv (a^{(p_i-1)})^c \equiv 1^c \equiv 1 \mod p_i
\]

Since we picked \(p_i\) arbitrarily from the set of prime factors of \(b\), this holds for all such \(p_i\).

3 Chinese Remainder Theorem Practice

In this question, you will solve for a natural number \(x\) such that,

\[
x \equiv 2 \pmod{3} \\
x \equiv 3 \pmod{5} \\
x \equiv 4 \pmod{7}
\]

(a) Suppose you find 3 natural numbers \(a, b, c\) that satisfy the following properties:

\[
a \equiv 2 \pmod{3} ; a \equiv 0 \pmod{5} ; a \equiv 0 \pmod{7},
\]
\[
b \equiv 0 \pmod{3} ; b \equiv 3 \pmod{5} ; b \equiv 0 \pmod{7},
\]
\[
c \equiv 0 \pmod{3} ; c \equiv 0 \pmod{5} ; c \equiv 4 \pmod{7}.
\]

Show how you can use the knowledge of \(a, b\) and \(c\) to compute an \(x\) that satisfies (1).

In the following parts, you will compute natural numbers \(a, b\) and \(c\) that satisfy the above 3 conditions and use them to find an \(x\) that indeed satisfies (1).

(b) Find a natural number \(a\) that satisfies (2). In particular, an \(a\) such that \(a \equiv 2 \pmod{3}\) and is a multiple of 5 and 7. It may help to approach the following problem first:

(b.i) Find \(a^*\), the multiplicative inverse of \(5 \times 7\) modulo 3. What do you see when you compute \((5 \times 7) \times a^*\) modulo 3, 5 and 7? What can you then say about \((5 \times 7) \times (2 \times a^*)\)?

(c) Find a natural number \(b\) that satisfies (3). In other words: \(b \equiv 3 \pmod{5}\) and is a multiple of 3 and 7.

(d) Find a natural number \(c\) that satisfies (4). That is, \(c\) is a multiple of 3 and 5 and \(\equiv 4 \pmod{7}\).

(e) Putting together your answers for Part (a), (b), (c) and (d), report an \(x\) that indeed satisfies (1).
Solution:

(a) Observe that \(a + b + c \equiv 2 + 0 + 0 \pmod{3}\), \(a + b + c \equiv 0 + 3 + 0 \pmod{5}\) and \(a + b + c \equiv 0 + 0 + 4 \pmod{7}\). Therefore \(x = a + b + c\) indeed satisfies the conditions in (1).

(b) This question asks to find a number \(0 \leq a < 3 \times 5 \times 7\) that is divisible by 5 and 7 and returns 2 when divided by 3. Let’s first look at Part (b.i):

(b.i) Observe that \((5 \times 7) \equiv 35 \equiv 2 \pmod{3}\). Multiplying both sides by 2, this means that \(2 \times (5 \times 7) \equiv 4 \pmod{3}\). So, the multiplicative inverse of \(5 \times 7\), \(a^*\) is exactly 2. To verify this: observe that \((5 \times 7) \times 2 = 70 = 3 \times 23 + 1\). Therefore \((5 \times 7) \times 2 \equiv 1 \pmod{3}\).

Consider \(5 \times 7 \times a^*\). Since it is a multiple of 5 and 7, it is equal to 0 modulo either of these numbers. On the other hand, \(5 \times 7 \times (2 \times a^*) \equiv 1 \times 2 \pmod{3}\), for the same reason that \(a^*\) is defined to be the multiplicative inverse of \(5 \times 7\) modulo 3.

Indeed observe that \(5 \times 7 \times (2 \times a^*) = 140\) precisely satisfies the criteria required in Part (b). It is equivalent to 0 modulo 5 and 7 and \(\equiv 2 \pmod{3}\).

(c) Let’s try to use a similar approach as Part (b). In particular, first observe that \(3 \times 7 \equiv 21 \equiv 1 \pmod{5}\). Therefore, \(b^*\), the multiplicative inverse of \(3 \times 7\) modulo 5 is in fact 1! So, let us consider \(3 \times 7 \times (3 \times b^*) = 63\): this is a multiple of 3 and 7 and is therefore 0 modulo both these numbers. On the other hand, \(3 \times 7 \times (3 \times b^*) \equiv 3 \pmod{5}\) for the reason that \(b^*\) is the multiplicative inverse of \(3 \times 7\) modulo 5.

(d) Yet again the approach of Part (b) proves to be useful! Observe that \(3 \times 5 \equiv 15 \equiv 1 \pmod{7}\). Therefore, \(c^*\), the multiplicative inverse of \(3 \times 5\) modulo 7 turns out to be 1. So, let us consider \(3 \times 5 \times (4 \times c^*) = 60\): this is a multiple of 3 and 5, is therefore 0 modulo both these numbers. On the other hand, \(3 \times 5 \times (4 \times c^*) \equiv 4 \pmod{7}\) for the reason that \(c^*\) is the multiplicative inverse of \(3 \times 5\) modulo 7.

(e) From Parts (b), (c) and (d) we find a choice of \(a, b, c\) (respectively = 140, 63, 60) which satisfies (2), (3) and (4). Together with Part (a) of the question, this implies that \(x = a + b + c = 263\) satisfies the required criterion in (1).

To verify this: observe that,

\[
\begin{align*}
263 &= 87 \times 3 + 2, \\
263 &= 52 \times 5 + 3, \\
263 &= 37 \times 7 + 4.
\end{align*}
\]