Practice Problems

Question 1. Using the Prime Number Theorem, estimate the number of prime numbers between 2 million and 7 million.

Solution:

The number of primes between 2000000 and 7000000
\[ \pi(7000000) - \pi(1999999) \approx \frac{7000000}{\log(7000000)} - \frac{1999999}{\log(1999999)} \approx 306274. \]

The exact answer is 327715, so we are about 6.5% out.

Question 2.

(a) Calculate \( \varphi(n) \) for \( n = 1200 \) and \( n = 2008 \).

(b) Let \( n \in \mathbb{N} \) and let \( p \) be a prime. Show that if \( p \mid n \) then \( \varphi(np) = p\varphi(n) \). Hint: consider the prime factorization of \( n \).

Solution:

(a)
\[ \varphi(1200) = \varphi(2^4 \cdot 3 \cdot 5^2) = \varphi(2^4) \cdot \varphi(3) \cdot \varphi(5^2) = (2^4)(2 \cdot 3^0)(4 \cdot 5^1) = 320 \]
\[ \varphi(2008) = \varphi(2^3 \cdot 251) = \varphi(2^3) \cdot \varphi(251) = (2^3)(1 \cdot 2^2)(250) = 1000 \]

(b) Since \( p \mid n \), the prime factorization of \( n \) is
\[ n = p^{e_1} p_1^{e_2} \cdots p_k^{e_k}, \]
for some \( k \). Thus
\[ \varphi(n) = \varphi(p^e) \varphi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = (p - 1)p^{e-1} \varphi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) \]
\[ \varphi(np) = \varphi(p^{e+1} p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = \varphi(p^{e+1}) \varphi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = (p - 1)p^e \varphi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = p \varphi(n) \]

Question 3.

(a) Show that the inverse of 5 modulo 101 is 5^{99}.

(b) Use repeated squaring to simplify \( 5^{99} \mod 101 \).

(c) Hence solve the equation \( 5x \equiv 31 \mod 101 \).
Solution: (a) By Fermat’s Little Theorem,
\[ 5^{100} \equiv 1 \pmod{101}, \]
so
\[ 5^{99} \cdot 5 \equiv 5 \cdot 5^{99} \equiv 1 \pmod{101}, \]
which by definition means that \( 5^{99} \) is the inverse of 5 modulo 101.

(b) \( 5^2 = 25, \ 5^4 = 19, \ 5^8 = 192 \equiv 58, \ 5^{16} = 58^2 \equiv 31, \)
\( 5^{32} \equiv 31^2 \equiv 52, \ 5^{64} \equiv 52^2 \equiv 78 \pmod{101}. \) Thus
\[ 5^{99} = 5^{64+32+2+1} \]
\[ \equiv 5^{64} \cdot 5^{32} \cdot 5^2 \cdot 5^1 \pmod{101} \]
\[ \equiv 78 \cdot 52 \cdot 25 \cdot 5 \pmod{101} \]
\[ \equiv 81 \pmod{101} \]
(c) \( x \equiv 5^{-1} \cdot 31 \equiv 81 \cdot 31 \equiv 87 \pmod{101}. \)

Check: \( 5 \cdot 87 = 435 \equiv 31 \pmod{101}. \)

Question 4. Find the two smallest positive integer solutions to the following system of equivalences
\[ x \equiv 2 \pmod{5} \]
\[ x \equiv 5 \pmod{8} \]
\[ x \equiv 4 \pmod{37} \]

Solution: This is a direct application of the CRT: We have \( m_1 = 5, \ m_2 = 8, \ m_3 = 37, \) so
\[ M_1 = 8 \cdot 37 = 296 \quad M_2 = 5 \cdot 37 = 185 \quad M_3 = 5 \cdot 8 = 40 \]
\[ M_1 \equiv 1 \pmod{5} \quad M_2 \equiv 1 \pmod{8} \quad M_3 \equiv 3 \pmod{37} \]
We have \( 1 \cdot 1 \equiv 1 \pmod{5} \quad 1 \cdot 1 \equiv 1 \pmod{8} \quad 3 \cdot 25 \equiv 1 \pmod{37}, \)
so \( N_1 = 1, \ N_2 = 1, \ N_3 = 25, \)
Thus \( x \equiv 2 \cdot 296 \cdot 1 + 5 \cdot 185 \cdot 1 + 4 \cdot 40 \cdot 25 = 5517 \equiv 1077 \pmod{5 \cdot 8 \cdot 37}. \) An integer satisfies the system of congruences if it is in this congruence class modulo \( 5 \cdot 8 \cdot 37 = 1480. \) The two smallest positive integers in this congruence class are 1077 and 2557.

Question 5.

(a) Calculate \( \varphi(27) \) and list the elements of \( (\mathbb{Z}/27\mathbb{Z})^\times. \)

(b) Find the order of 2 and 8, and state which one is a primitive root.

(c) Using this primitive root, find \( x \in (\mathbb{Z}/27\mathbb{Z})^\times \) such that \( x^7 \equiv 13 \pmod{27}. \)

Solution: \( \varphi(27) = \varphi(3^3) = 2 \cdot 3^2 = 18 \) and
\( (\mathbb{Z}/27\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}. \)

(b)

| \( n \) | \( 1 \) | \( 2 \) | \( 3 \) | \( 4 \) | \( 5 \) | \( 6 \) | \( 7 \) | \( 8 \) | \( 9 \) | \( 10 \) | \( 11 \) | \( 12 \) | \( 13 \) | \( 14 \) | \( 15 \) | \( 16 \) | \( 17 \) | \( 18 \) |
| \( 2^n \) | 2 | 4 | 8 | 16 | 5 | 10 | 20 | 13 | 26 | 25 | 23 | 19 | 11 | 22 | 17 | 7 | 14 | 1 |
| \( 8^n \) | 8 | 10 | 26 | 19 | 17 | 1 | 8 | 10 | 26 | 19 | 17 | 1 | 8 | 10 | 26 | 19 | 17 | 1 |
Thus $2$ has order $18 = \varphi(27)$ and is a primitive root, while $8$ has order $6$ and is not a primitive root.

(c) From the above table, $13 \equiv 2^8 \pmod{27}$. Since $2$ is a primitive root and $x \in (\mathbb{Z}/27\mathbb{Z})^*$, $x$ is some power of $2 \pmod{27}$. So let $x = 2^y$. Then

$$x^7 \equiv 13 \pmod{27}$$

becomes

$$(2^y)^7 = 2^{7y} \equiv 2^8 \pmod{27}.$$ 

Then since $2$ has order $\varphi(27) = 18$,

$$7y \equiv 8 \pmod{18}.$$ 

Multiplying both sides by $13$ (find by trial and error or Euclid’s algorithm) gives $y \equiv 14 \pmod{18}$, which we substitute back to get $x \equiv 2^{14} \equiv 22 \pmod{27}$. 
Assignment Problems

Question 1.

(a) Calculate $13^{2010} \pmod{71}$.
(b) Calculate $100^{-1} \pmod{2011}$.
(c) Calculate $\varphi(2010)$.

Solution:

(a) 30
(b) 181
(c) 528.

Question 2. Your Facebook friend posts the RSA public key $(N = 3551, e = 1565)$, hoping for secret messages from fans of repeated squaring. While looking through their rubbish, you find a scrap of paper with the number 67 on it, one of your favourite primes. You instantly know that it is significant. Find your friend’s private key.

Solution: The significance of 67 is that it is a factor of $N = 3551$, and using it we obtain the prime factorization of $N$, namely $N = 53 \cdot 67$. Thus $\varphi(N) = 52 \cdot 66 = 3432$. The private key, $d$, is the inverse of $e = 1565$ modulo 3432. We find it using Euclid’s algorithm:

\[
\begin{array}{c|cc}
3432 & 1 & 0 \\
2 & 1565 & 0 & 1 \\
5 & 302 & 1 & -2 \\
5 & 55 & -5 & 11 \\
2 & 27 & 26 & -57 \\
27 & 1 & -57 & 125 \\
0 & & & \\
\end{array}
\]

Thus the private key is 125.

Question 3. Find the smallest positive integer $x$ satisfying the following system, or show that no such $x$ exists:

\[
\begin{align*}
2x & \equiv 1 \pmod{3} \\
3x & \equiv 2 \pmod{5} \\
4x & \equiv 3 \pmod{7} \\
5x & \equiv 4 \pmod{11}
\end{align*}
\]

Hint: First multiply the first equation by $2^{-1}$, the second by $3^{-1}$ etc.

Solution: $2^{-1} \equiv 2 \pmod{3}, 3^{-1} \equiv 2 \pmod{5}, 4^{-1} \equiv 2 \pmod{7}, 5^{-1} \equiv 9 \pmod{11}$, so the system becomes

\[
\begin{align*}
x & \equiv 2 \pmod{3} \\
x & \equiv 4 \pmod{5} \\
x & \equiv 6 \pmod{7} \\
x & \equiv 3 \pmod{11}
\end{align*}
\]

We solve this via the CRT: $x \equiv 839 \pmod{1155}$. So the smallest positive solution is $x = 839$. 

Question 4. Define a function \( f: \mathbb{Z} \to \mathbb{N} \cup \{0\} \) by:

\[
\begin{cases}
  2n, & \text{if } n \geq 0 \\
  -1 - 2n, & \text{if } n < 0
\end{cases}
\]

Prove that \( f \) is a bijection. Give a formula for \( f^{-1}(m) \).

Solution: \( f \) is injective: Note that \( f(n) \) is even if \( n \geq 0 \) and is odd if \( n < 0 \). Thus if \( f(n) = f(m) \), either both \( m, n \geq 0 \), or both \( m, n < 0 \). In the first case \( 2m = f(m) = f(n) = 2n \) so \( m = n \). In the second case \( -1 - 2m = f(m) = f(n) = -1 - 2n \) so \( 2m = 2n \) so \( m = n \). Thus \( f(n) = f(m) \iff n = m \) in all cases.

\( f \) is surjective: Let \( N \in \mathbb{N} \cup \{0\} \). If \( N \) is even, let \( N = 2n \) for integer \( n \geq 0 \). Then \( f(n) = 2n = N \). If \( N \) is odd, let \( N = 2k - 1 \) for some positive integer \( k \). Then \( f(-k) = -1 - 2(-k) = 2k - 1 = N \). So in all cases, given \( N \in \mathbb{N} \cup \{0\} \) there exists \( m \in \mathbb{Z} \) with \( f(m) = N \).

Since \( k = (N + 1)/2 \), this analysis shows:

\[
 f^{-1}(n) = \begin{cases} 
  n/2, & \text{if } n \text{ is even} \\
  -(n + 1)/2, & \text{if } n \text{ is odd.}
\end{cases}
\]

Check: \( f^{-1}: \mathbb{N} \cup \{0\} \to \mathbb{Z} \) is a well defined function. If \( n \in \mathbb{N} \cup \{0\} \) is even then \( f(f^{-1}(n)) = f(n/2) = 2(n/2) = n \). If \( n \in \mathbb{N} \cup \{0\} \) is odd then \(- (n + 1)/2 \) is a negative integer and \( f(f^{-1}(n)) = f(- (n + 1)/2) = -1 - 2(- (n + 1)/2) = -1 + n + 1 = n \), so \( f \circ f^{-1} = 1_{\mathbb{N} \cup \{0\}} \).

Similarly, if \( n \in \mathbb{Z} \) and \( n \geq 0 \) then \( f(n) = 2n \) is even and \( f^{-1}(f(n)) = f^{-1}(2n) = (2n)/2 = n \). If \( n \in \mathbb{Z} \) and \( n < 0 \) then \( f(n) = -1 - 2n \) is odd and \( f^{-1}(f(n)) = f^{-1}(-1 - 2n) = -(1 - 2n + 1)/2 = 2n/2 = n \). So \( f^{-1} \circ f = 1_{\mathbb{Z}} \).

Question 5. Let \( A \) and \( B \) be sets and let \( g: A \to B \) be a function. A function \( f: B \to A \) is a left inverse for \( g \) if \( f \circ g = 1_A \). A function \( h: B \to A \) is a right inverse for \( g \) if \( g \circ h = 1_B \).

(a) Show that \( g \) has a left inverse iff it is injective.
(b) Show that \( g \) has a right inverse iff it is surjective.

Solution: (a) \( \Rightarrow \) If \( g: A \to B \) has a left inverse \( f: B \to A \) then \( f \circ g = 1_A \). If \( g(a) = g(b) \) then \( a = 1_A(a) = (f \circ g)(a) = f(g(a)) = f(b) = (f \circ g)(b) = 1_A(b) = b \), so \( g \) is injective.

\( \Leftarrow \) Fix \( a_0 \in A \). If \( g \) is injective, for each \( b \in A \) there is at most one \( a \in A \) with \( g(a) = b \). Define \( f: B \to A \) by

\[
f(b) = \begin{cases} 
  a, & \text{if there exists } a \text{ with } g(a) = b \\
  a_0, & \text{if there is no } a \text{ with } g(a) = b.
\end{cases}
\]

Then \( f(g(a)) = f(b) \) where \( g(a) = b \), so \( f(b) = a \) by definition. Hence for all \( a \in A \) we have \( (f \circ g)(a) = f(g(a)) = a = 1_A(a) \), so \( f \circ g = 1_A \), so \( g \) has left inverse \( f \). Notice that \( a_0 \) plays no role.

(b) \( \Rightarrow \) Suppose \( g: A \to B \) has a right inverse \( h: B \to A \), so \( g \circ h = 1_B \). Let \( b \in A \), and let \( a = h(b) \). Then \( g(a) = g(h(b)) = (g \circ h)(b) = 1_B(b) = b \), so \( g \) is surjective.

\( \Leftarrow \) Suppose \( g \) is surjective. Then for each \( b \in A \) there exists (at least one) \( a \in A \) with \( g(a) = b \). For each \( b \), choose a corresponding element \( a_b \) such that \( g(a_b) = b \). Now define \( h: B \to A \) by \( h(b) = a_b \). Then \( (g \circ h)(b) = g(h(b)) = g(a_b) = b \) for all \( b \in A \), so \( g \circ h = 1_B \), and \( g \) has right inverse \( h \).

In this direction we are required to make a simultaneous choice of \( a_b \) for each \( b \); this is allowed according to the Axiom of Choice in Set Theory (see Math 3306).

Question 6. Let \( G = \mathbb{Z} \times \mathbb{Q} \). Binary operations \( \ast, \circ \) and \( \bullet \) are defined on \( G \) as follows:
(a) \((a, b) \star (c, d) = (a + c, 2^c b + d)\);  
(b) \((a, b) \circ (c, d) = (a + c, 2^{-c} b + d)\);  
(c) \((a, b) \bullet (c, d) = (a + c, 2^c b - d)\).

Determine if \(\star\), \(\circ\), and \(\bullet\) are associative. For the associative operations, determine if there is an identity element.

**Solution:** All three are binary operations on \(G\).

Check associativity:

\[
\begin{align*}
(a, b) \star (c, d) \star (e, f) &= (a + c, 2^c b + d) \star (e, f) = (a + c + e, 2^c (2^e b + d) + f) \\
&= (a + c + e, 2^c + c + e b + 2^e d + f).
\end{align*}
\]

\[
\begin{align*}
(a, b) \star ((c, d) \star (e, f)) &= (a, b) \star (c + e, 2^e d + f) = (a + c + e, 2^c + c + e b + 2^e d + f).
\end{align*}
\]

\[
\begin{align*}
(a, b) \circ (c, d) \circ (e, f) &= (a + c, 2^{-c} b + d) \circ (e, f) = (a + c + e, 2^{-c} (2^e b + d) + f) \\
&= (a + c + e, 2^{-c} + c e b + 2^e d + f).
\end{align*}
\]

\[
\begin{align*}
(a, b) \circ ((c, d) \circ (e, f)) &= (a, b) \circ (c + e, 2^e d + f) = (a + c + e, 2^{-c} + c e b + 2^e d + f).
\end{align*}
\]

\[
\begin{align*}
(a, b) \bullet (c, d) \bullet (e, f) &= (a + c, 2^c b - d) \bullet (e, f) = (a + c + e, 2^c (2^e b - d) - f) \\
&= (a + c + e, 2^c + c e b - 2^e d - f).
\end{align*}
\]

\[
\begin{align*}
(a, b) \bullet ((c, d) \bullet (e, f)) &= (a, b) \bullet (c + e, 2^e d - f) = (a + c + e, 2^c + c e b - (2^e d - f)) \\
&= (a + c + e, 2^c + c e b - 2^e d + f).
\end{align*}
\]

So \(\bullet\) is not associative.

Check identity:

If \((a, b) \star (c, d) = (a, b)\) then \(a + c = a, 2^c b + d = d\) so \(c = 0\) and \(d = b\) so \(d = 0\). So if there is an identity, it must be \((0, 0)\). Check: \((a, b) \star (0, 0) = (a + 0, 2^0 b + 0) = (a, b)\) and \((0, 0) \star (a, b) = (0 + a, 2^0 a 0 + b) = (a, b)\). So \((0, 0)\) is the identity.

If \((a, b) \circ (c, d) = (a, b)\) then \(a + c = a, 2^{-c} b + d = d\) so \(c = 0\) and \(d = b\) so \(d = 0\). So if there is an identity, it must be \((0, 0)\). Check: \((a, b) \circ (0, 0) = (a + 0, 2^0 b + 0) = (a, b)\) and \((0, 0) \circ (a, b) = (0 + a, 2^{-a} 0 + b) = (a, b)\). So \((0, 0)\) is the identity.