Show all your work. Justify your solutions. Answers without justification will not receive full marks.

Only hand in the problems on page 2.

Practice Problems

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

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.

Question 3.

(a) Show that the inverse of 5 modulo 101 is 5^{99}.
(b) Use repeated squaring to simplify $5^{99} \pmod{101}$.
(c) Hence solve the equation $5x \equiv 31 \pmod{101}$.

Question 4. Find the two smallest positive integer solutions to the following system of equivalences

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 5 \pmod 8 \\ x &\equiv 4 \pmod{37} \end{aligned}$$

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

Assignment Problems

Question 1.

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

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.

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

$$\begin{aligned} 2x &\equiv 1 \pmod{3} \\ 3x &\equiv 2 \pmod{5} \\ 4x &\equiv 3 \pmod{7} \\ 5x &\equiv 4 \pmod{11} \end{aligned}$$

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

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

$$f(n) = \begin{cases} 2n, & \text{if } n \geq 0 \\ -1 - 2n, & \text{if } n < 0 \end{cases}$$

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

Question 5. Let A and B be sets and let $g\colon A \to B$ be a function. A function $f\colon B \to A$ is a *left inverse* for g if $f \circ g = 1_A$. A function $h\colon B \to A$ 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.

Question 6. Let $G = \mathbb{Z} \times \mathbb{Q}$. Binary operations $\star$, $\circ$ 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.