Problems marked with an asterisk (*) are compulsory for only the students who are registered in Math 377. The bonus problem will count as extra credit for everyone. However, no help on the bonus problem will be given during office hours, nor should you seek help at the math help desk.

(1) Consider the ring \( \mathbb{Z}[\sqrt{-118}] \). Show that
\[
343 = 7^3 = (15 + \sqrt{-118})(15 - \sqrt{-118})
\]
are two different factorizations of 343 into irreducibles. (Hint: you’ll want to use norms, introduced in Assignment 1).

(2) (*) An ideal \( I \) of a ring \( R \) is said to be irreducible if it cannot be written nontrivially as the intersection of two other ideals.
(a) Show that if an ideal \( I \) in the ring of integers of a number field admits a non-trivial factorization \( I = I_1I_2 \), then \( I \) is properly contained in both \( I_1 \) and \( I_2 \). Conclude that \( I \) is irreducible if the quotient \( R/I \) is a field.
(b) Use part (a) to express \( 343 = 7^3 \) into a product of irreducible ideals in \( \mathbb{Z}[\sqrt{-118}] \).
(c) Show that the cube of the ideal \( I = (7, 15 + \sqrt{-118}) \) is principal.

(3) Compute the greatest common divisor of \( a = 9 + 49i \) and \( b = 31 + 39i \) in the ring \( \mathbb{Z}[i] \), and express the result as a linear combination of \( a \) and \( b \) with coefficients in \( \mathbb{Z}[i] \).

(4) (a) Find \( \gcd(31463, 9782) \), and express it in terms of 31463 and 9782.
(b) Find \( \gcd(100!, 3^{100}) \).

(5) Prove that every number \( n \geq 12 \) can be written in the form \( 3a + 7b \), with \( a, b \in \mathbb{Z}_{\geq 0} \).

(6) Define \( \text{lcm}(a, b) = ab/\gcd(a, b) \).
(a) Show that \( \text{lcm}(a, b) \) is a multiple of \( a \), and also a multiple of \( b \).
(b) Show that if \( a|n \) and \( b|n \), then \( \text{lcm}(a, b)|n \).

(7) (a) Solve \( 59x \equiv 5000 \pmod{999} \).
(b) Find all solutions to the equation \( \phi(x) = 24 \). Do the same for \( \phi(x) = 14 \).

(8) (a) Let
\[
\binom{p}{k} = \frac{p!}{k!(p-k)!}
\]
be a binomial coefficient, and suppose that \( p \) is a prime. If \( 1 \leq k \leq p-1 \), show that \( p \) divides \( \binom{p}{k} \). Deduce that \( (a+1)^p \equiv a^p + 1 \pmod{p} \).
(b) Use part (a) to give another proof of Fermat’s little theorem, \( a^{p-1} \equiv 1 \pmod{p} \) if \( p \nmid a \).

**Bonus.** Find all strictly increasing functions \( f : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0} \) such that \( f(2) = 2 \), and whenever \( \gcd(m, n) = 1 \), then \( f(mn) = f(m)f(n) \).