1. (10 points) Let $p \in \mathbb{N}$ be a prime. The order mod $p$ of an integer $x \in \mathbb{Z}$, $x \not\equiv 0 \pmod{p}$, is the smallest number $d \in \mathbb{N}$ such that $x^d \equiv 1 \pmod{p}$—it is denoted $\text{ord}_p(x)$. By Fermat’s little theorem, the order exists.

(a) Show that if $x \equiv y \pmod{p}$, then $\text{ord}_p(x) = \text{ord}_p(y)$. Thus we may talk about the order of a nonzero congruence class $\bar{x} \in \mathbb{Z}/p$.

Solution. We have shown that for any polynomial $f$ with integer coefficients, $f(a) \equiv f(b) \pmod{p}$ if $a \equiv b \pmod{p}$. Take $f(t) = t^d$.

More explicitly, if $x \equiv y \pmod{p}$, then $x = y + np$ for some $n \in \mathbb{Z}$. Then by the binomial theorem,

$$x^d \equiv (y + np)^d \equiv \sum_{i=0}^{d} \binom{d}{i} (np)^i y^{d-i} \equiv y^d \pmod{p}$$

since every term other than the $i = 0$ term is divisible by $p$.

(b) Show that for any nonzero $\bar{x} \in \mathbb{Z}/p$, $\text{ord}_p(\bar{x}) | p - 1$

Solution. We can write $p - 1 = dq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < p - 1$. Since $x^{p-1} \equiv (x^d)^q \cdot x^r \equiv x^r \equiv 1 \pmod{p}$, we must have $r = 0$ since $d$ is the smallest integer $\geq 1$ with $x^d \equiv 1 \pmod{p}$.

(c) Show that for any $d | p - 1$, there are precisely $d$ congruence classes $\bar{x} \in \mathbb{Z}/p$ such that $\text{ord}_p(\bar{x}) | d$.

Solution. We have seen that the polynomial $t^{p-1} - 1$ factorizes mod $p$ as

$$t^{p-1} - 1 = \prod_{a \in (\mathbb{Z}/p)^*} (t - a)$$

If $d | p - 1$, then $t^d - 1 | t^{p-1} - 1$, so $t^d - 1$ factorizes into $d$ distinct linear factors mod $p$. Every element of order dividing $d$ is a root of this polynomial.
(d) Show that \( \text{ord}_{101}(2) = 100 \).

**Solution.** The order must be 2, 4, 5, 10, 20, 25, 50, or 100. We could compute these powers, but it’s enough to just show that \( 2^{20} \not\equiv 1 \mod 101 \) and \( 2^{50} \not\equiv 1 \mod 101 \) since every proper divisor of 100 divides 20 or 50. Indeed, \( 2^{10} \equiv 32^2 \equiv 1024 \equiv 14 \mod 101 \), and \( 2^{20} \equiv 49 \cdot 4 \equiv -6 \mod 101 \), so \( 2^{50} \equiv (2^{20})^2 \cdot 2^{10} \equiv 36 \cdot 14 \equiv 4 \cdot 25 \equiv -1 \mod 101 \). Thus \( \text{ord}_{101}(2) = 100 \).

2. (10 points) Let \( m, n \in \mathbb{N} \) with \( d = \gcd(m, n) \), and \( a, b \in \mathbb{Z} \).

(a) Show that there is a solution to the simultaneous system:

\[
\begin{align*}
x &\equiv a \mod m \\
x &\equiv b \mod n
\end{align*}
\]

if and only if \( a \equiv b \mod d \).

**Solution.** (\( \Rightarrow \)) If there is a solution \( x \), then \( m|x - a \) and \( n|x - b \). \( d \) divides \( m \) and \( n \), so it divides \( (x - a) - (x - b) = b - a \).

(\( \Leftarrow \)) There is a solution to \( d = mu + nv \). If \( a = b + qd \), take \( x = a + qmu \).

*Note:* We could have also used the Chinese remainder theorem to analyze the above system mod every prime power, though it would have been messier.

(b) If there is a solution, show that it is unique mod \( \text{lcm}(m, n) \).

**Solution.** If \( x, y \) are solutions then \( m|x - y \) and \( n|x - y \), and therefore \( \text{lcm}(m, n)|x - y \).

3. (10 points) Find all solutions to the following congruences mod \( n \).

(a) \( 15x \equiv 25 \mod 70 \) (\( n = 70 \)).

**Solution.** \( \gcd(15, 25, 70) = 5 \), so this congruence is equivalent to \( 3x \equiv 5 \equiv -9 \mod 14 \), and thus \( x \equiv -3 \mod 14 \). There are then 5 lifts mod 70: \( x \equiv -3, 11, 25, 39, 53 \mod 70 \).

(b) \( x^2 + 3x + 2 \equiv 5 \mod 15 \) (\( n = 15 \)).

**Solution.** Using the Chinese remainder theorem, this is equivalent to the system:

\[
\begin{align*}
x^2 + 3x + 2 &\equiv 5 \mod 5 \\
x^2 + 3x + 2 &\equiv 5 \mod 3
\end{align*}
\]

The former is \( (x + 1)(x + 2) \equiv 0 \mod 5 \) and has solutions \( x \equiv -1, -2 \mod 5 \); the latter is \( x^2 \equiv 0 \mod 3 \) and has a unique solution \( x \equiv 0 \mod 3 \). Using the Chinese remainder theorem again, there are two solutions: \( x \equiv 3, 9 \mod 15 \).
(c) Solve the following simultaneous system of congruences \((n = 63 = 3^2 \cdot 7)\)

\[
10x \equiv -7 \mod 21 \\
6x \equiv 21 \mod 27
\]

**Solution.** By the Chinese remainder theorem, this system is equivalent to:

\[
10x \equiv -7 \mod 3 \iff x \equiv -1 \mod 3 \\
10x \equiv -7 \mod 7 \iff x \equiv 0 \mod 7 \\
6x \equiv 21 \mod 27 \iff 2x \equiv 7 \mod 9 \iff x \equiv -1 \mod 9
\]

The last inequality implies the first, and again by the Chinese remainder theorem there is a unique solution mod \(9 \cdot 7\): \(x = 35 \mod 63\). \(\square\)

4. (15 points) We’ve seen how our knowledge of the arithmetic of \(\mathbb{Z}[i]\) allows us to solve \(n = x^2 + y^2\). In this problem we’ll start (to finish in a future homework) studying \(\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} | a, b \in \mathbb{Z}\} \subset \mathbb{C}\) to understand solutions to \(n = x^2 + 2y^2\). Recall that you’ve proven previously that \(R = \mathbb{Z}[\sqrt{-2}]\) is a Euclidean domain and thus has unique factorization.

(a) Prove the units are \(R^* = \{\pm 1\}\).

**Solution.** If \(\alpha = x + y\sqrt{-2} \in R^*\), then for some \(\beta \in R\), \(\alpha \beta = 1\), so \(|\alpha|^2 \cdot |\beta|^2 = 1\) and thus \(|\alpha|^2 = 1\). But \(|\alpha|^2 = x^2 + 2y^2 = 1\) only for \(\alpha = \pm 1\) (since \(|\cdot|^2\) is nonnegative). Clearly both are indeed units. \(\square\)

(b) Prove that if we have \(\alpha \in R\) with \(|\alpha|^2 = p\) prime, then \(\alpha\) is prime as an element of \(R\). (Hint: Recall irreducibles are prime in Euclidean domains.)

**Solution.** If \(\alpha = \beta \gamma\), then \(p = |\beta|^2 |\gamma|^2\), so either \(|\beta|^2 = 1\) or \(|\gamma|^2 = 1\), and therefore \(\alpha\) is irreducible, by (a). \(\square\)

(c) Note that the prime factorization of 2 is \(-\sqrt{-2} \cdot \sqrt{-2}\). Prove that if \(p \in \mathbb{N}\) is an odd prime number, the prime factorization of \(p\) in \(R\) is either \(p = p\) (\(p\) remains prime) or \(p = \pi \overline{\pi}\) for distinct (non-associate) primes \(\pi, \overline{\pi} \in R\).

**Solution.** Suppose \(p\) does not remain prime; then it has some proper prime divisor \(\pi \in R\). Since \(p\) is real, \(\overline{\pi}\) must also be a divisor, and therefore \(\pi \overline{\pi} = |\pi|^2\) is a divisor of \(p\). Thus, for some \(x + y\sqrt{-2} \in R\), \((x + y\sqrt{-2})|\pi|^2 = p\), which clearly requires \(y = 0\), so \(|\pi|^2 |p\) and thus \(\pi \overline{\pi} = p\). It remains to show that \(\pi \not\sim \overline{\pi}\) if \(|\pi|^2 \neq 2\), and this follows immediately from \(R^* = \{\pm 1\}\) since the imaginary part of \(\pi\) must be nonzero. \(\square\)

(d) Let \(p \in \mathbb{N}\) be an odd prime. Considering \(p \in R\), show that \(p\) remains prime if and only if \(x^2 + 2 \equiv 0 \mod p\) has no solution.
 Solution. We did this in class: \((\iff)\) If \(p = \pi \pi\), then \(p = x^2 + 2y^2\) has a solution. Clearly \(p \nmid x\) or else \(p|y\) also and therefore \(p^2|x^2 + 2y^2 = p\). Thus, \(x^2 + 2y^2 \equiv 0 \mod p\) and \(x,y \not\equiv 0 \mod p\), so \((x/y)^2 + 2 \equiv 0 \mod p\).

\((\Rightarrow)\) Suppose \(p\) remains prime and there is some \(x \in \mathbb{Z}\) such that \(p|x^2 + 2\). Then \(p|(x + \sqrt{-2})(x - \sqrt{-2})\) so \(p\) divides one of them, which is a contradiction since we can’t have \(p(u + v\sqrt{-2}) = x \pm \sqrt{-2}\).

(e) Let \(p\) be an odd prime. Show that if \(x^2 + 2 \equiv 0 \mod p\) has a solution (we’ll see later this happens iff \(p \equiv 1,3 \mod 8\)) then there is a unique solution to \(p = x^2 + 2y^2\) (we consider \((\pm x, \pm y)\) to all be the same solution).

Solution. First, \(p = \pi \pi\), so if \(\pi = x + y\sqrt{-2}\), we know \(p = x^2 + 2y^2\). If \(p = u^2 + 2v^2\), then \(\alpha = u + v\sqrt{-2}\) divides \(p\) in \(r\), and thus \(\alpha = \pi\) or \(\pi\), since \(\alpha\) cannot be a unit.

5. (10 points) Answer the following questions with either true (T) or false (F).

(a) \[\text{There is a unique pair of numbers } a, b \in \mathbb{N} \text{ with } \gcd(a, b) = 4 \text{ and } \text{lcm}(a, b) = 56 \text{ (}(a, b) \text{ and } (b, a) \text{ are counted as the same pair).}\]

Solution. False. There are two: \((4, 56)\) and \((28, 8)\).

(b) \[\text{There is a unique solution mod 3 to } 6x - 1 \equiv 3 \mod 9.\]

Solution. False. There is no solution; this equation is equivalent to \(6x \equiv 4 \mod 9\) and \(\gcd(6, 9) = 3 \not\mid 4\).

(c) \[\text{For all } a, b, c \in \mathbb{N}, \gcd(a, \text{lcm}(b, c)) = \text{lcm}(\gcd(a, b), \gcd(a, c)).\]

Solution. True. It’s enough to show that for each prime \(p\) the power of \(p\) appearing in the factorization on each side is the same. Supposing the maximal powers of \(p\) dividing \(a, b, c\) are \(\alpha, \beta, \gamma\), then the power of \(p\) on the left is \(\min(\alpha, \max(\beta, \gamma))\) and that on the right is \(\max(\min(\alpha, \beta), \min(\alpha, \gamma))\) which are clearly equal.

(d) \[\text{For all } x \in \mathbb{Z}, x^7 \equiv x \mod 21.\]

Solution. True. Certainly \(x^7 \equiv x \mod 7\). Also, \(x^3 \equiv x \mod 3\), so \(x^7 \equiv x^3 \cdot x^3 \cdot x \equiv x^3 \equiv x \mod 3\), and by the Chinese remainder theorem \(x^7 \equiv x \mod 21\).

(e) \[\text{For } a, b, c \in \mathbb{Z}, \text{ if } a|c \text{ and } b|c \text{ then } ab|c.\]

Solution. False. \(6|18\) and \(9|18\) but \(54 \not\mid 18\).
(f) \( 5^{175} \equiv 17 \mod 19 \).

*Solution.* \( 301 \equiv -5 \mod 19 \), so \( 5^{175} \equiv 5^{-4} \mod 19 \). The inverse of \( 5 \mod 19 \) is 4, so \( 5^{-4} \equiv 4^4 \equiv 16^2 \cdot 4 \equiv (-3)^2 \cdot 4 \equiv 17 \mod 19 \). 

\[ \square \]

(g) \( \) There are infinitely many primes \( p \in \mathbb{N} \) for which \( p^2 + 2 \) is also prime.

*Solution.* \( \) For \( p \neq 3 \), \( p \) is \( \pm 1 \mod 3 \) so \( p^2 \equiv 1 \mod 3 \) and \( p^2 + 3 \) is divisible by 3.

\[ \square \]

(h) \( \) For \( a \in \mathbb{N} \) and \( f(t) \) a polynomial with integer coefficients, \( \gcd(a, f(a)) = \gcd(a, f(0)) \).

*Solution.* \( \) If \( f(t) = \sum \lambda_ix^i \), then successively applying \( \gcd(a, f(a)) = \gcd(a, f(a) - \lambda_na^n) \) we are left with \( \gcd(a, f(a)) = \gcd(a, f(0)) \).

\[ \square \]

(i) \( \) There are infinitely many primes \( p \) such that \( p + 4 \) and \( p + 8 \) are prime.

*Solution.* \( \) 0, 4, 8 are representatives of all congruence classes \( \mod 3 \), so one of \( p, p + 4, p + 8 \) is divisible by 3.

\[ \square \]

(j) \( \) There are exactly 2 solutions \( \mod n \) to \( x^2 + 5x + 1 \equiv 0 \mod n \) for \( n = 3^{341} \cdot 5^{500} \).

*Solution.* \( \) Using the Chinese remainder theorem, there are two solutions \( \mod 15 \) since \( x^2 + 5x + 1 \equiv (x + 2)(x - 2) \mod 5 \) and \( x^2 + 5x + 1 \equiv (x + 1)^2 \mod 3 \). Lifting fails in the latter case, because for \( f = x^2 + 5x + 1 \), \( f'(-1) \equiv 0 \mod 3 \) but \( f'(-1)/3 \equiv -1 \mod 3 \). Indeed we can see directly that \( x^2 + 5x + 1 \equiv 0 \mod 9 \) has no solutions by evaluating at lifts of \(-1\): \((-1)^2 + 5(-1) + 1 \equiv -3 \neq 0 \mod 9\), \((2)^2 + 5(2) + 1 \equiv 15 \neq 0 \mod 9\), \((-4)^2 + 5(-4) + 1 \equiv -3 \neq 0 \mod 9\).

\[ \square \]