SPRING 2025: MATH 540 EXAM I

You must provide all details to receive full credit. No calculators are allowed on this exam. Please put your name on all pages that you turn in.

Statements. Define any terms you use in the statements below. (3 points each)

1. State the Fundamental Theorem of Arithmetic.

Solution. Every integer greater than one can be written uniquely (up to order) as a product primes numbers.

Comment The uniqueness part of the theorem is crucial, and took a substantial amount of work to establish.

2. State the Division Algorithm.

Solution. Given non-zero integers a, b, with $a > 0$, there exist unique integers q, r such that $b = aq + r$, with $0 \leq r < a$.

4. State Euler's Theorem.

Solution. If we let $\phi(n)$ denote the Euler totient function, the $\phi(n)$ is the number of positive integers less than n and relatively prime to n. Euler's theorem states that if $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \bmod n$.

3. Let X be a set with relation $\sim$. Define what it means for $\sim$ to be an equivalence relation. For $x \in X$, define $[x]$, the equivalence class of x and state a fundamental property of equivalence classes.

Solution. To be an equivalence relation, $\sim$ must satisfy: (i) $x \sim x$; (ii) If $x \sim y$, then $y \sim x$; (iii) If $x \sim y$ and $y \sim z$, then $x \sim z$, for all $x, y, z \in X$. Given $x \in X$, the equivalence class of x is the et $[x] : -\{x' \in X \mid x \sim x'\}$. Given any two equivalence classes $[x], [x']$, either $[x] = [x']$ or $[x] \cap [x'] = \emptyset$.

5. If $n = p_1^{e_1} \cdots p_r^{e_r}$ is a prime factorization, what are the values of $\tau(n)$ and $\sigma(n)$, where $\tau(n)$ denotes the number of divisors of n, and $\sigma(n)$ denotes the sum of the divisors of n?

Solution. $\tau(n) = (e_1 + 1) \cdots)e_r + 1)$ and $\sigma(n) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{e_r+1} - 1}{p_r - 1}$.

Calculations (10 points each)

1. Wilson's theorem states that the positive integer p is prime if and only if $(p-1)! \equiv -1 \bmod p$. Verify Wilson's theorem for $p = 13$.

Solution. Working modulo 13, we have

$$\begin{aligned} 12! &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \\ &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot (-6) \cdot (-5) \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) \\ &\equiv 120 \cdot 6 \cdot (-6) \cdot (-120) \\ &\equiv 3 \cdot 6 \cdot (-6) \cdot (-3) \\ &\equiv 18 \cdot 18 \\ &\equiv 5 \cdot 5 \\ &\equiv 12 \\ &\equiv -1. \end{aligned}$$

2. Use the identification $\mathbb{Z}_n \to \mathbb{Z}_a \times \mathbb{Z}_b$, for $n = ab$, with $\gcd(a, b) = 1$, given in class to find all solutions in $\mathbb{Z}_{15}$ to the equation $x^2 \equiv 4 \bmod 15$.

Solution. In this case, we have the correspondence $\mathbb{Z}_{15} \xrightarrow{f} \mathbb{Z}_3 \times \mathbb{Z}_5$. Note that both 2 and square to 4 mod 3, since 4 is congruent to 1 mod 3. Also, 2 and 3 square to 4 mod 5. Thus, in $\mathbb{Z}_3 \times \mathbb{Z}_5$, the ordered pairs (1, 2), (1, 3), (2,2), (2, 3) square to (4, 4) = (1, 4). Under the correspondence $f : 7 \to (1,2), 2 \to (2,2)$, $13 \to (1,3), 8 \to (2,3)$. Thus, mod 13, each of 7, 13, 2, 8 square to 4.

3. Find all solutions to $12x \equiv 20$ mod 28 in $\mathbb{Z}_{28}$ and $\mathbb{Z}$.

Solution. We first note that $12x \equiv 20$ mod 28 means that $12x - 20 = n28$, for some n. Thus, $3x - 5 = n7$, so that $3x \equiv 5$ mod 7. Multiplying this equivalence by 5, we get $x \equiv 25 \equiv 4$ mod 7, so that $x = 4$ is a solution to the original congruence equation. The other solutions are of the form $4 + \frac{28}{4} \cdot k$, with $1 \leq k \leq 3$, so we get that the full set of solutions are: 4, 11, 18, 25, modulo 28. Over $\mathbb{Z}$, the solutions are: $\{7n + 4 \mid n \in \mathbb{Z}\}$.

Comment Note that it looks like we divided the original congruence equation by 4, but strictly speaking, we did not do this, since 4 is not a unit mod 28. We translated the congruence equation to an integer equation, and then divided by 4, and then transcribed the new integer equation to a congruence equation mod 7.

4. Verify Euler's product formula and Gauss's theorem for $n = 1,224$.

Comment. Verifying Euler's formula is not too difficult for 1224, however, I did not realize that 1224 has 24 divisors, and thus one must calculate $\phi(d)$ for 24 values, then add. SO: everyone got full value for this problem.

5. Simplify 11^{183} mod 124.

Solution. Note that $\gcd(11, 124) = 1$, so we may apply Euler's theorem to conclude $11^{\phi(124)} \equiv 1$ mod 124. Here

$$\phi(124) = \phi(2^2 \cdot 31) = \phi(2^2) \cdot \phi(31) = 2 \cdot 30 = 60.$$

On the other hand, $183 = 60 \cdot 3 = \phi(124) \cdot 3$. Thus, modulo 124 we have,

$$11^{183} \equiv 11^{\phi(124)} \cdot 11^3 \equiv 121 \cdot 11 \equiv -3 \cdot 11 \equiv -33 \equiv 91.$$

Induction, well ordering and equivalence relations. (5 points each)

1. Use the Well Ordering Principle as stated in class to show that if $S \subseteq \mathbb{Z}$ is bounded below, then S has a least element.

Solution. If $S \subseteq \mathbb{N}$, then S has a least element by the Well Ordering Principle. If S contains negative integers, let b be a lower bound and consider the set $S' := \{s + |b| \mid s \in S\}$, i.e., S shifted $|b|$ units to the right. Then $S' \subseteq \mathbb{N}$, so that S' has a least element s_0', by the Well Ordering Principle. Then $s_0 := s_0' - |b|$ is a least element for S.

2. Use mathematical induction to prove that $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$, for all $n \geq 0$.

Solution. When $n = 0$, the left hand side of the sum is 1, and the right hand side is $2^1 - 1 = 1$, so the base case holds. Suppose the statement is true for $n - 1$ Then, $1 + 2 + \cdots + 2^{n-1} = 2^n - 1$. Adding 2^n to both sides of this equation we get

$$1 + 2 + \cdots 2^{n-1} + 2^n = 2^n + 2^n - 1 = 2 \cdot 2^n - 1 = 2^{n+1} - 1,$$

which is what we want.

3. Let X be the non-zero integers and define $a \sim b$ if and only if $ab > 0$, for $a, b \in X$. Show that this gives and equivalence relation on X and identify the equivalence classes.

Solution. If $a \in X$, then $a \cdot a = a^2 > 0$, so $a \sim a$. If $a \sim b$, then $ab > 0$, so $ba > 0$, hence $b \sim a$. Suppose $a \sim b$ and $b \sim c$. Then $ab > 0$ and $bc > 0$. Then a, b are both positive, or a, b are both negative. Similarly, b, c are both positive or both negative. Suppose a, b are both positive. Then c must be positive, and thus, $ac > 0$, so $a \sim c$. The argument is similar if a, b are both negative. Therefore, $a \sim c$.

Now, any two positive integers are equivalent to each other and any two negative integers are equivalent to each other. Thus, there are just two equivalence classes, namely, [1] and [−1].

Proof problem. Give a rigorous proof of the fact that every positive integer can be written as a product of prime numbers, i.e., the existence part of the Fundamental Theorem of Arithmetic. (20 points)

Solution. Suppose the theorem is false. We seek a contradiction. Let X denote the set of positive integers that cannot be written as a product of primes. By assumption, $X \neq \emptyset$. Thus, by the Well ordering Principle, X has a least element a. By definition of X, x is not prime. Thus, $a = bc$, for positive integers strictly less than a. Since a is the least element in X, $b, c \not{i}nX$. Thus, b is a product of primes and c is a product of primes. Therefore, $bc = a$ is a product of primes, contrary to $a \in X$. Thus, every positive integer is a product of primes.

Comment. A very similar proof can be given using induction.

Optional bonus problems. Solutions to bonus problems must be essentially completely correct to receive any credit.

1. Let $p > 2$ be a prime. Show that the equation $x^2 \equiv 1 \bmod p$ has exactly two solutions in $\mathbb{Z}_p$. (10 points)

Solution. Clearly 1, -1 satisfy the equation $x^2 \equiv 1 \bmod p$. It's important to note that since $p > 2$, $1 \not\equiv 1 \bmod p$, so these are two distinct solutions. Now suppose $a^2 \equiv 1 \bmod p$. Then $(a+1)\cdot(a-1) \equiv 0 \bmod p$. Thus, in $\mathbb{Z}$, $p \mid (a+1)(a-1)$. Since p is prime, $p \mid a+1$ or $p \mid a-1$. But then, $a \equiv -1 \bmod p$ or $a \equiv 1 \bmod p$, which gives what we want.

2. Show that a positive integer n is not prime if and only if $\phi(n) \leq n - \sqrt{n}$. (10 points)

Solution. Suppose n is not prime. We can write $n = p_1^{e_1} \cdots p_r^{e_r}$, where $p_1 < p_2 < \cdots < p_r$, with $r = 1$ and $e \geq 2$ or $r > 1$ and each $e_i \geq 1$. We claim $\sqrt{n} \geq p_1$. Suppose this is true. Then we have $1 - \frac{1}{p_1} \leq 1 - \frac{1}{\sqrt{n}}$. If $r = 1$ and $e \geq 2$, we have $\phi(n) = n(1 - \frac{1}{p_1}) \leq n(1 - \frac{1}{\sqrt{n}}) \leq n - \sqrt{n}$. Suppose $r > 1$ and each $e_i \geq 1$. Then

$$\phi(n) = n \cdot (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}) \leq n \cdot (1 - \frac{1}{p_1}) \leq n \cdot (1 - \frac{1}{\sqrt{n}}) = n - \sqrt{n},$$

Note that the first inequality follows from the fact that each $1 - \frac{1}{p_i} < 1$.

To prove the claim, suppose $n = p^e$, with $e \geq 2$. Then clearly, $\sqrt{n} \geq p$. Suppose $r > 1$. Then

$$\sqrt{n} \geq p_1^{\frac{e_1}{2}} \cdot p_2^{\frac{e_2}{2}} = \sqrt{p_1}\sqrt{p_2} \cdot p_1^{\frac{e_1-1}{2}} p_2^{\frac{e_2-1}{2}} \geq \sqrt{p_1}\sqrt{p_1} = p_1.$$

For the converse, suppose $n = p$ is prime. Then $\phi(n) = n - 1 < n - \sqrt{n}$, which gives what we want.

3. Prove that if $\gcd(a, b) = 1$, then $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \bmod ab$. (10 points)

Solution. We use the correspondence from class: $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$. Note that, taking canonical images under f, we have,

$$f(a^{\phi(b)} + b^{\phi(a)}) = (a^{\phi}(b) + b^{\phi(a)}, a^{\phi(b)} + b^{\phi(a)}) = (b^{\phi(a)}, a^{\phi(b)}) = (1, 1),$$

the last equality following from Euler's theorem. Since $f(1) = (1, 1)$ and f is a one-to-one function, we must have $1 = a^{\phi(b)} + b^{\phi(a)}$ in $\mathbb{Z}_{ab}$, i.e., $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \bmod ab$.