Practice Exams

Exam 1 Sample A

---

1. Write down the prime factorization of 10!.

2. Find the least non-negative residue of $11^{67} \mod 13$.

3. Find all incongruent solutions $\mod 40$, as least non-negative residues, to the following lienar congruence:

$$12x \equiv 28 \mod 40$$

4. Use the Euclidean Algorithm to find $\gcd(390, 72)$ and write this as a linear combination of the two.

5. Use the Chinese Remainder Theorem to find the smallest positive solution to the system:

$$\begin{aligned} x &\equiv 2 \mod 5 \\ x &\equiv 1 \mod 6 \\ x &\equiv 4 \mod 7 \end{aligned}$$

6. Use mathematical induction to prove that:

$$n! \geq n^3 \text{ for } n \geq 6$$

7. Determine if the following sets are well-ordered or not. You may assume only that $\mathbb{Z}^+$ is well-ordered.

$$\begin{aligned} S_1 &= [0, 1] \cap \mathbb{Q} \\ S_2 &= \{1 - 2^k \mid k \in \mathbb{Z}^+\} \end{aligned}$$

8. Use the Fundamental Theorem of Arithmetic (uniqueness of prime factorization) to prove that $\sqrt{2}$ is irrational. Hint: Use contradiction.

9. Suppose $a, b, c, d \in \mathbb{Z}$ with $a \mid c$, $b \mid c$, $d = \gcd(a, b)$, and $d^2 \mid c$. Prove that $ab \mid c$.

Exam 1 Sample B

---

1. (a) Find $\pi(18)$.
   (b) Show that the set $\{\frac{a}{b} \mid a, b \in \mathbb{Z}^+, a > b\}$ is not well-ordered.
   (c) Find how many primes there are, approximately, between one billion and two billion.
2. Find the number of zeros at the end of 1000! with justification.
3. The following are all false. Provide explicit numerical counterexamples.
   (a) $a \mid bc$ implies $a \mid b$ or $a \mid c$.
   (b) $a \mid b$ and $a \mid c$ implies $b \mid c$.
   (c) $3 \mid a$ and $3 \mid b$ implies $\gcd(a, b) = 3$.
4. Simplify $\prod_{j=1}^{n} \left(1 + \frac{2}{j}\right)$. Your result should not have a $\prod$ in it, or any sort of long product.
5. Use Mathematical Induction to prove $2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 2$ for all integers $n \geq 1$.
6. Find all $n \in \mathbb{Z}$ with $n^2 - 5n + 6$ prime.
7. Suppose p is a prime and a is a positive integers less than p. Find all possibilities for $\gcd(a, 7a + p)$.
8. Use the Fundamental Theorem of Arithmetic to prove that $\sqrt{6}$ is irrational.
9. Prove that for $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ that if $a^n \mid b^n$ then $a \mid b$.

Exam 2 Sample A

---

1. Show that 91 is a Fermat Pseudoprime to the base 3. Note that 91 is not prime!
2. Prove that if $n \geq 2$ and $\gcd(6, n) = 1$ then $\phi(3n) = 2\phi(2n)$.
3. Classify all numbers n for which $\tau(n) = 12$.
4. Suppose n is a perfect number and p is a prime such that pn is also perfect. Prove $\gcd(p, n) \neq 1$.
5. Prove that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \bmod ab$ if $\gcd(a, b) = 1$.

6. Suppose that p is prime and $n \in \mathbb{Z}^+$. Prove that $p \nmid n$ iff $\phi(pn) = (p-1)\phi(n)$.

7. (a) Show that 3 is a primitive root modulo 17.

   (b) Find all primitive roots modulo 17.

8. A partial table of indices for 7, a primitive root of 13 is given here:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_7 a$	12	b	8	10	3	7	a	9	4	2	5	6

   (a) Find a and b.

   (b) Use the table to solve the congruence $3^{x-1} \equiv 5 \bmod 13$.

   (c) Use the table to solve the congruence $4x^5 \equiv 11 \bmod 13$.

9. Suppose $\text{ord}_p a = 3$, where p is an odd prime. Show $\text{ord}_p(a+1) = 6$.

10. Suppose r is a primitive root modulo m, and k is a positive integers with $\gcd(k, \phi(m)) = 1$ Prove r^k is also a primitive root.

Exam 2 Sample B

---

1. Calculate:

   (a) $\phi(2^3 \cdot 5 \cdot 11^2)$

   (b) $\sigma(200)$

   (c) $\tau(2000)$

2. Use Wilson's Theorem to find the remainder when 16! is divided by 19.

3. Find all n with $\phi(n) = 16$.

4. Show that 25 is a Fermat Pseudoprime to the base 7.

5. An abundant number is a number n with $sigma(n) > 2n$. Prove that there are infinitely many even abundant numbers by finding on eabundant number and by showing that if n is abundant and a prime p satisfies $p \nmid n$ then pn is also abundant.

6. A partial table of indices for 2, a primitive root of 13, is given here:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_2 a$	12	1	4	2	9	5	11	3	a	b	7	6

   (a) Find a and b with justification.

(b) Use the table to solve the congruence $3^{2x+1} \equiv 9 \bmod 13$.

(c) Use the table to solve the congruence $7x^5 \equiv 3 \bmod 13$.

7. Prove that if $\mathrm{ord}_n a = hk$ then $\mathrm{ord}_n(a^h) = k$.

8. Let r be a primitive root for an odd prime p. Prove that $\mathrm{ind}_r(p-1) = \frac{1}{2}(p-1)$.

9. Find all positive integers n such that $\phi(n)$ is prime. Explain!

10. Show that if a is relatively prime to m and $\mathrm{ord}_m a = m - 1$ then m is prime.

Final Exam Sample A

---

1. Given $A = 6259162$ and $B = 206346$.

   (a) Find the prime factorizations of A and B and use them to find $\gcd(A, B)$.

   (b) Find $\gcd(A, B)$ using the Euclidean Algorithm.

2. Use the Chinese Remainder Theorem to find the smallest and second smallest nonnegative solutions to the system:

$$x \equiv 2 \bmod 5$$
$$x \equiv 5 \bmod 8$$
$$x \equiv 15 \bmod 17$$

3. For each of $n = 19, 309, 5672, 37699$ find the exact value p_n of the n^{th} prime (however you want) and then approximate value a_n of the n^{th} prime (using the Prime Number Theorem Corollary). Calculate the percentage error

$$\frac{100|p_n - a_n|}{p_n}$$

   for each.

4. Find all incongruent solutions mod 124 to the linear system:

$$52x \equiv 4 \bmod 124$$

5. Find all primitive roots for $n = 13$ as follows: First find the smallest positive primitive root. Then use the Theorem from class which yields all the remaining ones. Final answers should be least nonnegative residues.

6. It's a fact that $r = 6$ is a primitive root mod 11.

(a) Use this to construct a table of indices for this primitive root.

(b) Use the table of indices to solve the equation: $x^8 \equiv 5 \bmod 11$. Your answer(s) should be mod 11.

(c) Use the table of indices to solve the equation: $3^x \equiv 5 \bmod 11$. Your answer(s) should be mod 10.

7. Calculate the following Jacobi symbols:

   (a) $\left(\frac{1141}{667}\right)$

   (b) $\left(\frac{1141}{51127}\right)$

8. Suppose you intercept the following ciphertext from Alice to Bob:

   `2982 2237 3239 1364 8541 7043`

   You know that Bob's public key is $(e, n) = (1655, 11639)$. Bob thinks this is secure because he doesn't believe that his n can be factored easily. Factor $n = 11639$, find $\phi(n)$, find d and then decrypt the message. Be clear about the steps you take.

9. Determine if each of the following sets is well-ordered. If a set is not well-ordered give evidence. If a set is well-ordered no evidence is required.

   (a) $\{0\} \cup \{(n+4)/n \mid n \in \mathbb{Z}^+\}$

   (b) $2\mathbb{Z}$

   (c) $\{\lfloor \sqrt{n} \rfloor \mid n \in \mathbb{Z}^+\}$

10. Suppose $p \geq 11$ is an unknown prime. Find all solutions to $x^2+8 \equiv 6x \bmod p$. Note that your solutions will be mod p.

11. Consider the inequality:

    $$3^n < n!$$

    (a) Find the smallest positive integer n_0 for which this is true. Do this however you wish.

    (b) Prove by induction that $3^n < n!$ for all $n \geq n_0$.

12. Suppose p is an odd prime such that there is some a so that a is a quadratic residue of p but $2a$ is a quadratice non-residue of p. Prove that $p \equiv \pm 3 \bmod 8$.

13. Prove that for $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ that if $a^n \mid b^n$ then $a \mid b$.

14. Prove that if $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$ and $c \mid (a+b)$ then $\gcd(c, a) = \gcd(c, b) = 1$.