Math 351 Midterm

Due Monday, November 28 at 5pm

This is a out-of-class exam. You can work with a group on any problem worth at least 15 points, but on the problems worth either 5 or 10 points you are not to talk about the problem with anyone (except me). If you do work as a group on a problem, clearly state on your paper who is in your group. You should turn in NO MORE than 100 points worth of problems, and I will be grading the test as if it were based on 100 total points. There are 5, 10, 15, 20, 40, and 50 point problems. In general, the more points, the harder the problem (in some cases the scale is exponential, not linear). Throughout the test **R**, **C**, **Q** and **Z** are the real numbers, complex numbers, the rational numbers, and the integers, respectively. If you have questions, you can come to my office hours or ask me via e-mail. Solutions should be written in LaTeX or Markdown and converted to a PDF. There are 36 questions for a total of 420 points to choose from. Good luck!

1. (15 points) Let $a, b \in \mathbf{Z}$. In class we defined $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$ such that

   $$\overline{a} = \{z \in \mathbf{Z} \mid \text{ the remainders of } a \text{ and } z \text{ are the same when divided by } n\}.$$

   Show the following statements are equivalent.

   (1) $\overline{a} = \overline{b}$ as elements in $\mathbf{Z}/n\mathbf{Z}$;

   (2) $a + n\mathbf{Z} = b + n\mathbf{Z}$ (Here $c + n\mathbf{Z} := \{c + z \mid z \in n\mathbf{Z}\}$);

   (3) $a - b \in n\mathbf{Z}$;

   (4) There exists $q_1, q_2, r \in Z$, $0 \leqslant r < n$, such that

   $$\begin{aligned} a &= q_1 n + r \\ b &= q_2 n + r. \end{aligned}$$

2. (5 points) Use the prime enumeration sieve to make a list of all primes up to 100.

3. (5 points) Let $\psi(x)$ be the number of primes of the form $4k-1$ that are $\leq x$. Use a computer to make a conjectural guess about $\lim_{x\to\infty} \psi(x)/\pi(x)$. You must explain your reasoning and give any code you might have used.

4. (5 points) In the following parts, assume that $y = 10000$.

   (1) Compute $\pi(y) = \#\{\text{primes } p \leq y\}$.

   (2) The prime number theorem implies $\pi(x)$ is asymptotic to $\dfrac{x}{\log(x)}$. How close is $\pi(y)$ to $y/\log(y)$?

5. (15 points) Let a, b, c, d, and m be integers. Prove that

   (1) if $a \mid b$ and $b \mid c$ then $a \mid c$.

   (2) if $a \mid b$ and $c \mid d$ then $ac \mid bd$.

   (3) if $m \neq 0$, then $a \mid b$ if and only if $ma \mid mb$.

   (4) if $d \mid a$ and $a \neq 0$, then $|d| \leq |a|$.

6. (5 points) (a) (Do this part by hand.) Compute the greatest common divisor of 323 and 437 using the division algorithm (i.e., do not just factor a and b).

   (b) Compute by any means the greatest common divisor of

$$31415926535897932384626433$$

   and

$$2718281828459045235360287 47.$$

7. (10 points) Suppose p is a prime and a and k are positive integers. Prove that if $p \mid a^k$, then $p^k \mid a^k$.

8. (10 points) (a) Prove that if a positive integer n is a perfect square, then n cannot be written in the form $4k + 3$ for k an integer.

   (b) Prove that no integer in the sequence

$$11, 111, 1111, 11111, 111111, \ldots$$

   is a perfect square. (Hint: $111 \cdots 111 = 111 \cdots 108 + 3 = 4k + 3$.)

9. (10 points) Prove that for any positive integer n, the set $(\mathbf{Z}/n\mathbf{Z})^*$ under multiplication modulo n is a group.

10. (5 points) Compute the following gcd's using Euclid's Algorithm:

$$\gcd(15, 35) \quad \gcd(247, 299) \quad \gcd(51, 897) \quad \gcd(136, 304)$$

11. (5 points) Use the Extended Euclidean Algorithm to find x, $y \in \mathbf{Z}$ such that $2261x + 1275y = 17$.

12. (10 points) Prove that if a and b are integers and p is a prime, then $(a + b)^p \equiv a^p + b^p \pmod{p}$. You may assume that the binomial coefficient

$$\binom{p}{r} = \frac{p!}{r!(p-r)!}$$

is an integer.

13. (15 points) (1) Prove that if x, y is a solution to $ax + by = d$, with $d = \gcd(a, b)$, then for all $c \in \mathbf{Z}$,

$$x' = x + c \cdot \frac{b}{d}, \qquad y' = y - c \cdot \frac{a}{d} \tag{1}$$

   is also a solution to $ax + by = d$.

   (2) Find two distinct solutions to $2261x + 1275y = 17$.

   (3) Prove that all solutions are of the form (1) for some c.

14. (5 points) Let $f(x) = x^2 + ax + b \in \mathbf{Z}[x]$ be a quadratic polynomial with integer coefficients, for example, $f(x) = x^2 + x + 6$. Formulate a conjecture about when the set

$$\{f(n) : n \in \mathbf{Z} \text{ and } f(n) \text{ is prime}\}$$

is infinite. Give numerical evidence that supports your conjecture.

15. (5 points) Find four complete sets of residues modulo 7, where the ith set satisfies the ith condition: (1) nonnegative, (2) odd, (3) even, (4) prime.

16. (20 points) Define a sequence of decimal integers a_n as follows: $a_1 = 0$, $a_2 = 1$, and a_{n+2} is obtained by writing the digits of a_{n+1} immediately followed by those of a_n. For example, $a_3 = 10$, $a_4 = 101$, and $a_5 = 10110$. Determine the n such that a_n is a multiple of 11, as follows:

(a) Find the smallest integer $n > 1$ such that a_n is divisible by 11.

(b) Prove that a_n is divisible by 11 if and only if $n \equiv 1 \pmod 6$.

17. (15 points) (1) Prove that φ is multiplicative as follows. Suppose m, n are positive integers and $\gcd(m, n) = 1$. Show that the natural map $\psi : \mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ is an injective homomorphism of rings, hence bijective by counting, then look at unit groups.

    (2) Prove conversely that if $\gcd(m, n) > 1$, then the natural map $\psi : \mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ is not an isomorphism.

18. (40 points) Suppose b is any integer that is relatively prime to h, $1 \leqslant h \leqslant 72$. If $x \geqslant 106706$, then the interval $(x, 1.048x]$ contains a prime congruent to b modulo h.

19. Show that if p is a positive integer such that both p and $p^2 + 2$ are prime, then $p = 3$.

20. (5 points) Let $\varphi : \mathbf{N} \to \mathbf{N}$ be the Euler φ function.

    (1) Find all natural numbers n such that $\varphi(n) = 1$.

    (2) Do there exist natural numbers m and n such that $\varphi(mn) \neq \varphi(m) \cdot \varphi(n)$?

21. (5 points) Find a formula for $\varphi(n)$ directly in terms of the prime factorization of n.

22. (5 points) Is the set $\mathbf{Z}/5\mathbf{Z} = \{0, 1, 2, 3, 4\}$ with binary operation multiplication modulo 5 a group? If so, prove it. If not, show why.

23. (10 points) Find all *four* solutions to the equation

$$x^2 - 1 \equiv 0 \pmod{35}.$$

24. (10 points) Prove that for any positive integer n the fraction $(12n + 1)/(30n + 2)$ is in reduced form.

25. (10 points) Suppose a and b are positive integers.

    (1) Prove that $\gcd(2^a - 1,\ 2^b - 1) = 2^{\gcd(a,b)} - 1$.

    (2) Does it matter if 2 is replaced by an arbitrary prime p?

    (3) What if 2 is replaced by an arbitrary positive integer n?

26. (10 points) For every positive integer b, show that there exists a positive integer n such that the polynomial $x^2 - 1 \in (\mathbf{Z}/n\mathbf{Z})[x]$ has at least b roots.

27. (15 points) (1) Prove that $(\mathbf{Z}/2^n\mathbf{Z})^*$ is generated by -1 and 5.

28. (15 points) Let p be an odd prime.

    (1) (*) Prove that there is a primitive root modulo p^2. (Hint: Use that if a, b have orders n, m, with $\gcd(n, m) = 1$, then ab has order nm.)

    (2) Prove that for any n, there is a primitive root modulo p^n.

    (3) Explicitly find a primitive root modulo 125.

29. (10 points) (*) In terms of the prime factorization of n, characterize the integers n such that there is a primitive root modulo n.

30. (10 points) Find the proportion of primes $p < 1000$ such that 2 is a primitive root modulo p.

31. (10 points) Find a prime p such that the smallest primitive root modulo p is 37.

32. (50 points) Suppose $a \in \mathbf{Z}$ is not -1 or a perfect square. Then there are infinitely many primes p such that a is a primitive root modulo p.

33. (5 points) This problem concerns encoding phrases using numbers. What is the longest that an arbitrary sequence of letters (no spaces) can be if it must fit in a number that is less than 10^{20}?

34. (15 points) For any $n \in \mathbf{N}$, let $\sigma(n)$ be the sum of the divisors of n; for example, $\sigma(6) = 1 + 2 + 3 + 6 = 12$ and $\sigma(10) = 1 + 2 + 5 + 10 = 18$. Suppose that $n = pqr$ with p, q, and r distinct primes. Devise an "efficient" algorithm that given n, $\varphi(n)$ and $\sigma(n)$, computes the factorization of n. For example, if $n = 105$, then $p = 3$, $q = 5$, and $r = 7$, so the input to the algorithm would be

$$n = 105, \qquad \varphi(n) = 48, \qquad \text{and} \quad \sigma(n) = 192,$$

and the output would be 3, 5, and 7.

35. (15 points) Using any language, implement Algorithm 2.3.13. Your code must be well indented and well documented.

36. (10 points) In this problem, you will "crack" an RSA cryptosystem. What is the secret decoding number d for the RSA cryptosystem with public key $(n, e) = (5352381469067, 4240501142039)$?

37. (10 points) Nikita creates an RSA cryptosystem with public key

$$(n, e) = (1433811615146881, 329222149569169).$$

In the following problem, show the steps you take to factor n. (Don't simply factor n directly using a computer.)

(1) Somehow you discover that $d = 116439879930113$. Show how to use the probabilistic algorithm (Algorithm 3.4.5) to factor n.