Number Theory
Spring 2018

Exam 1 Review

1 Topics

1.1 Definitions

Divides, divisor, complimentary divisor, factor, multiple, prime, composite, GCD, relatively prime, $\pi(x)$, congruence, congruence class, $\mathbb{Z}/n\mathbb{Z}$, arithmetic progression, group, abelian, ring, units, field

1.2 Results

Periodicity of GCD, Division Algorithm, (Extended) Euclidean Algorithm, Bézout's Lemma, Euclid's Lemma, Fundamental Theorem of Arithmetic, Infinitude of Primes, Sieve of Eratosthenes, Prime Number Theorem, relationship between $\mathbb{Z}/n\mathbb{Z}$ and remainders, modular arithmetic, $\mathbb{Z}/n\mathbb{Z}$ as a ring, connection between the ring $\mathbb{Z}/n\mathbb{Z}$ and modular arithmetic, $(\mathbb{Z}/n\mathbb{Z})^\times$, when $\mathbb{Z}/n\mathbb{Z}$ is a field

2 Exercises

Exercise 1. Prove that $6^n|(3n)!$ for all $n \in \mathbb{N}$.

Exercise 2. Compute $(344, 120)$ and express it as a linear combination of 344 and 120.

Exercise 3. Let a, b, $c \in \mathbb{Z}$. Prove that if $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.

Exercise 4. Two consecutive primes p and q are called *twin primes* if $q = p + 2$.[1] Three consecutive primes p, q and r are called *prime triplets* if $q = p + 2$ and $r = q + 2$. Prove that $(3, 5, 7)$ is the only prime triplet.

[1] It is conjectured (the *twin prime conjecture*) that there are infinitely many twin primes. In other words, it is believed that the difference between consecutive primes takes on the value 2 infinitely often. It is one of the most famous open problems in number theory. The current state of affairs (as of 2015) is the result that $\liminf_{n\to\infty}(p_{n+1} - p_n) < 246$, i.e. the difference between consecutive primes is less than 246 infinitely often.

Exercise 5. Prove the following alternate formulation of the Fundamental Theorem of Arithmetic. Every $n \in \mathbb{N}$ can be expressed in the form $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ where each p_i is prime and $m_i \in \mathbb{N}$. This expression is unique up to the order of the prime powers. [*Suggestion:* Use the original FTA to establish existence by grouping common primes together. Then prove uniqueness using a cancellation argument.]

Exercise 6. Let a, b, $n \in \mathbb{N}$. Prove that $a|b$ if and only if $a^n|b^n$. [*Suggestion:* For one direction use the Fundamental Theorem of Arithmetic.]

Exercise 7. Let $n \in \mathbb{N}$. Express the number of positive divisors of n as a function of the prime factorization of n.

Exercise 8. Let a, b, $c \in Z$. Prove that if $a^2 + b^2 = c^2$, then at least one of a or b is even. [*Suggestion:* Work modulo 4.]

Exercise 9. Find the inverse of $243 + 578\mathbb{Z}$ in $(\mathbb{Z}/578\mathbb{Z})^\times$.

Exercise 10. The International Standard Book Number (ISBN) consists of nine digits $a_1 a_2 \cdots a_9$ followed by a tenth "check digit" a_{10}, which satisfies

$$a_{10} = \sum_{k=1}^{9} k a_k \pmod{11}.$$

Show that if two (unequal) digits (among the first 9) of a valid ISBN are accidentally transposed, the check digit will detect this error.

Exercise 11. Prove that if $a \in \mathbb{Z}$ is odd, then for any $n \in \mathbb{N}$

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}.$$

Exercise 12.

Let p_n denote the nth prime number.

a. By taking the logarithm of both sides in the Prime Number Theorem and performing some algebra arrive at the limit

$$\lim_{x \to \infty} \frac{\log \pi(x)}{\log x} = 1.$$

b. Multiply and divide by $\log \pi(x)$ in the Prime Number Theorem, perform some algebra and use part **a** to show that

$$\lim_{x \to \infty} \frac{\pi(x) \log \pi(x)}{x} = 1.$$

c. Take $x = p_n$ in part **b** to conclude that

$$\lim_{n\to\infty} \frac{n \log n}{p_n} = 1,$$

i.e. the nth prime has size roughly $n \log n$, for large n.