Extension Material: Number Theory (Non-Assessable)

Note(s)

This handout is designed to offer students extended knowledge that complements the core course content. The material presented here goes beyond the foundational requirements of the course, delving into more advanced or specialized topics that may enhance your understanding of the subject.

While this information is not part of the course's examinable content, it may serve as a valuable resource for those who are curious to explore the subject in greater depth or wish to challenge themselves further. These topics are provided solely for your reference, and there is no obligation to study them for assessments or exams.

We encourage students who are interested in broadening their knowledge or seeking a deeper appreciation of the course concepts to review this handout at their own pace.

Basic Number Theory Concepts

Divisibility and Prime Numbers

Concept(s)

Divisibility: An integer a is divisible by an integer b if there exists an integer k such that $a = bk$.

Prime Numbers: A prime number is a positive integer greater than 1 that has exactly two factors: 1 and itself. Examples: 2, 3, 5, 7, 11, 13, 17, 19, ...

Greatest Common Divisor and Least Common Multiple

Concept(s)

Greatest Common Divisor (GCD): The largest positive integer that divides both numbers without a remainder.

Least Common Multiple (LCM): The smallest positive integer that is divisible by both numbers.

Relation: For positive integers a and b, we have:

$$\text{lcm}(a, b) \cdot \text{gcd}(a, b) = |ab|.$$

Intermediate Concepts

Modular Arithmetic

Concept(s)

Definition: $a =_{(m)} b$ means m divides $(a - b)$.

Properties: Preserves addition, subtraction, and multiplication.

Fermat's Little Theorem

Concept(s)

Statement: If p is prime and a is not divisible by p, then:

$$a^{p-1} =_{(p)} 1.$$

Advanced Concepts

Bézout's Identity

Please also refer to Extended Euclidean Algorithm.

Concept(s)

Statement: For integers a and b, there exist integers x and y such that:

$$ax + by = \gcd(a, b).$$

Primitive Roots

Concept(s)

Definition: We say g is a primitive root modulo n if for every a coprime to n, we have

$$g^k =_{(n)} a \text{ for some integer } k.$$

Quadratic Residues

Concept(s)

Definition: An integer a is a quadratic residue modulo n if there exists an x such that:

$$x^2 =_{(n)} a.$$

Fundamental Proofs

Exercise 1. Prove that if p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Answer(s)

Suppose $p \nmid a$. Then $\gcd(p, a) = 1$, so by Bézout's identity, there exist integers x and y such that:

$$px + ay = 1.$$

Multiplying both sides by b:

$$pxb + aby = b,$$

and since $p \mid ab$, we can write $ab = kp$ for some integer k. Substituting:

$$pxb + kpy = b,$$
$$p(xb + ky) = b.$$

This shows that $p \mid b$.

Exercise 2. Prove that for any integers a, b, and positive integer m:

$$\gcd(a, m) = \gcd(b, m) = 1 \implies \gcd(ab, m) = 1.$$

Answer(s)

By Bézout's identity, there exist integers x_1, y_1, x_2, y_2 such that:

$$ax_1 + my_1 = 1$$
$$bx_2 + my_2 = 1.$$

Multiplying these equations:

$$(ax_1 + my_1)(bx_2 + my_2) = 1.$$

Expanding:

$$abx_1x_2 + amx_1y_2 + bmy_1x_2 + m^2y_1y_2 = 1.$$

Rearranging:

$$abx_1x_2 + m(ax_1y_2 + by_1x_2 + my_1y_2) = 1.$$

This is of the form $abz + mw = 1$ for some integers z and w, which proves that $\gcd(ab, m) = 1$.

Advanced Proofs

Exercise 3. Prove that for any prime p and integer a not divisible by p:

$$a^{p-1} =_{(p)} 1.$$

Answer(s)

Consider the sequence $a, 2a, 3a, \ldots, (p-1)a$ modulo p. All these numbers are distinct modulo p (if $ia =_{(p)} ja$ for $i \neq j$, then $p \mid (i-j)a$, which is impossible as p is prime and doesn't divide a).

Therefore, this sequence is a permutation of $1, 2, \ldots, p-1$ modulo p. Multiplying all elements:

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a =_{(p)} 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1),$$
$$a^{p-1}(p-1)! =_{(p)} (p-1)!.$$

Since $(p-1)!$ is not divisible by p (Wilson's theorem), we can cancel it on both sides:

$$a^{p-1} =_{(p)} 1.$$

Exercise 4. Prove that for any prime p and integer a:

$$(a+1)^p =_{(p)} a^p + 1.$$

Answer(s)

Using the binomial theorem:

$$\begin{aligned}(a+1)^p &= \sum_{k=0}^{p} \binom{p}{k} a^k \\ &= a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k + 1.\end{aligned}$$

For $1 \leq k \leq p-1$, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is divisible by p. Therefore, all terms in the sum are $=_{(p)} 0$, leaving:

$$(a+1)^p =_{(p)} a^p + 1.$$

Exercise 5. Let p be an odd prime. Prove that:

$$\left(\frac{p-1}{2}\right)! =_{(p)} \pm 1.$$

Answer(s)

Consider the product of pairs $(1 \cdot (p-1)), (2 \cdot (p-2)), \ldots, (\frac{p-1}{2} \cdot \frac{p+1}{2})$ modulo p. Each pair multiplies to $=_{(p)} -1$, and there are $\frac{p-1}{2}$ pairs. Therefore ww have

$$1 \cdot 2 \cdot \ldots \cdot \tfrac{p-1}{2} \cdot \tfrac{p+1}{2} \cdot \ldots \cdot (p-1) =_{(p)} (-1)^{\frac{p-1}{2}}.$$

The left side is $(p-1)! =_{(p)} -1$ by Wilson's theorem. Hence, the following could be proved as

$$-1 =_{(p)} (-1)^{\frac{p-1}{2}},$$
$$\left(\left(\tfrac{p-1}{2}\right)!\right)^2 =_{(p)} (-1)^{\frac{p-1}{2}+1},$$
$$\left(\tfrac{p-1}{2}\right)! =_{(p)} \pm 1.$$

Challenging Problems

Exercise 6. Prove that for any odd prime p and any integer a not divisible by p, exactly one of $a^{\frac{p-1}{2}} =_{(p)} 1$ or $a^{\frac{p-1}{2}} =_{(p)} -1$ holds.

Answer(s)

By Fermat's Little Theorem, we know that $a^{p-1} =_{(p)} 1$. This means $(a^{\frac{p-1}{2}})^2 =_{(p)} 1$. Therefore, $a^{\frac{p-1}{2}}$ is a root of the quadratic congruence $x^2 =_{(p)} 1$. The only roots of this congruence are ± 1, so $a^{\frac{p-1}{2}} =_{(p)} \pm 1$. It can't be both, so exactly one of the two congruences holds.

Exercise 7. Prove that for any prime $p > 3$, $p^2 - 1$ is divisible by 24.

Answer(s)

For $p > 3$, p is of the form $6k \pm 1$ for some integer k.
Case 1: If $p = 6k + 1$, then:

$$p^2 - 1 = (6k + 1)^2 - 1 = 36k^2 + 12k = 12k(3k + 1).$$

Case 2: If $p = 6k - 1$, then:

$$p^2 - 1 = (6k - 1)^2 - 1 = 36k^2 - 12k = 12k(3k - 1).$$

In both cases, $p^2 - 1$ is divisible by 12. Also, in both cases, one of k or $3k \pm 1$ must be even, so $p^2 - 1$ is divisible by 24.

Exercise 8. Let p be an odd prime. Prove that:

$$1^p + 2^p + \ldots + (p-1)^p =_{(p)} 0.$$

Answer(s)

By Fermat's Little Theorem, for $1 \leq a < p$, we have $a^p =_{(p)} a$. Therefore:

$$1^p + 2^p + \ldots + (p-1)^p =_{(p)} 1 + 2 + \ldots + (p-1).$$

The sum on the right is $\frac{p(p-1)}{2}$ so

$$1^p + 2^p + \ldots + (p-1)^p =_{(p)} \frac{p(p-1)}{2} =_{(p)} 0,$$

since $\frac{p(p-1)}{2}$ is a multiple of p.

Additional Challenging Exercises

Note(s)

These exercises are designed to be extremely challenging and to encourage deep thinking about advanced number theory concepts. Students are encouraged to attempt these problems and discuss their approaches and partial solutions on the Ed Forum. Full solutions are not provided to promote independent problem-solving and collaborative discussion.

1. (Quadratic Reciprocity) For odd primes p and q, prove that:
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$
2. Prove that if p is a prime of the form $4k+1$, then p can be written as the sum of two squares.
3. (Primitive roots) Prove that if g is a primitive root modulo a prime p, then the order of g^k modulo p is $(p-1)/\gcd(k, p-1)$ for any integer k.
4. Prove that there are infinitely many primes of the form $4k+3$.
5. (Wilson's theorem generalization) For a positive integer n, prove that
$$(n-1)! =_n -1$$
if and only if n is prime.
6. Let p be an odd prime. Prove that
$$\sum_{k=1}^{p-1} k^{p-2} =_{(p)} 0.$$
7. Prove that for any integers a and b,
$$\gcd(a,b) \cdot \mathrm{lcm}(a,b) = |ab|.$$