Number Theory II: Congruences

Congruences are a simple, but extremely useful concept in number theory. The magic of congruences ("modular arithmetic") can often turn an otherwise complex and lengthy argument into a couple of lines. This handout summarizes the basic definitions and results about congruences that you need to know.

Definition

Definition: Let $a, b \in \mathbb{Z}$, and $m \in \mathbb{N}$. We say **"a is congruent to b modulo m"**, and write "$a \equiv b \mod m$", if $m \mid (a-b)$. The integer m is called the **modulus** of the congruence.

Equivalent definition: By the definition of divisibility, "$m \mid (a-b)$" means that there exists $k \in \mathbb{Z}$ such that $a - b = km$, i.e., $a = b + km$. Thus, the above definition can be stated as follows. *This version is particularly suited for proofs involving congruences.*

Definition: Let $a, b \in \mathbb{Z}$, and $m \in \mathbb{N}$. Then "$a \equiv b \mod m$" means that $a = b + km$ for some $k \in \mathbb{Z}$.

- **Examples:** $22 \equiv 4 \bmod 6$ (since $6 \mid (22-4)$), $4 \equiv -2 \bmod 6$ (since $6 \mid 4-(-2)$), $5 \equiv 1 \bmod 2$ (since $2 \mid (1-5)$).
- **Special case: Congruences modulo 2:** $n \equiv 0 \mod 2$ means that $n = 2k$ for some $k \in \mathbb{Z}$. But the integers of the form $n = 2k$ are exactly the even integers. Similarly, the integers satisfying $n \equiv 1 \bmod 2$ are those of the form $n = 1 + 2k$ for some $k \in \mathbb{Z}$, i.e., the odd integers.
- **Special case: Congruences to 0:** By the above definition, "$a \equiv 0 \bmod m$" means $m \mid (a-0)$, i.e., it is equivalent to the divisibility relation $m \mid a$.
- **Notes:**
  - *Congruences are only defined for integers, and the modulus m must be a natural number.* For example, $a \equiv 1/2 \mod 2$ is not defined since $1/2$ is not an integer; similarly, $a \equiv b \bmod 0$ is not defined since 0 is not a natural number.
  - *The modulus m is an essential part of the definition.* Make sure to always specify the modulus; saying "a is congruent to b", or writing "$a \equiv b$", without specifying a modulus, makes no sense.

Properties

What makes congruences so useful is that, to a large extent, they can be manipulated like ordinary equations. Congruences **to the same modulus** can be added, multiplied, and taken to a fixed positive integral power; i.e., for any $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$ we have:

- **Adding/subtracting congruences:** If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a + c \equiv b + d \bmod m$. and $a - c \equiv b - d \mod m$.
- **Multiplying congruences:** If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$.
- **Taking congruences to the k-th power:** If $a \equiv b \mod m$ and $k \in \mathbb{N}$, then $a^k \equiv b^k \mod m$.
- **Chaining congruences together:** If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.

- **Proofs.** Proving the above congruence properties is an instructive exercise in applying proof techniques you've learned earlier in this course, and you should be able to carry out such proofs. Some examples will be given in class or on worksheets; others will be assigned as homework.
- **Notes.**
  - *Congruences to different moduli can NOT be added, multiplied, etc.* In the above properties, the modulus m must be the same at each occurrence.
  - *Congruences can NOT be divided.* An analogous property involving division of congruences does not exist. This is because congruences are only defined for integers, and dividing congruences would introduce rational numbers.
  - *Congruences can NOT be exponentiated.* It is *not* true that $a \equiv b \mod m$ and $c \equiv d \mod m$ implies $a^c \equiv b^d \mod m$. (However, you can take each side of the congruence to the *same* exponent k: $a \equiv b \bmod m$ implies $a^k \equiv b^k \bmod m$.)

Famous Congruence: Fermat's Little Theorem

Fermat's Little Theorem: Let p be a prime and $a \in \mathbb{N}$ such that $p \nmid a$. Then $a^{p-1} \equiv 1 \mod p$.

- **Example:** The number 2017 is prime, so by Fermat's Little theorem, we have $a^{2016} \equiv 1 \mod 2017$ for any natural number a that is not divisible by 2017. In particular, it follows that each of the numbers $2^{2016} - 1, 3^{2016} - 1, \ldots, 2016^{2016} - 1$ is divisible by 2017.
- **Note:** The modulus, p, in this theorem must be a prime. For composite moduli the above congruence does, in general, not hold.

Division with Remainder

The familiar process of **division with remainder** is made precise in the following theorem.

Theorem (Division with Remainder (Division Algorithm)). Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then there exist unique integers q ("quotient") and r ("remainder") such that $a = qb + r$ and $0 \le r < b$.

- **Example:** If $a = 16$ and $b = 5$, then $16 = 3 \cdot 5 + 1$, so in this case $q = 3$ and $r = 1$. By the theorem, this is the only such representation with a remainder satisfying $0 \le r < 5$.
- **Congruences and remainders.** The remainder, r, in the division algorithm is the *smallest* nonnegative integer that is congruent to a modulo q.

Further Resources

In the text the above definitions and theorems can be found in Chapter 6:
Congruences: Definition 7.15, p. 142.
Addition/Multiplication Properties: Lemma 7.19, p. 145.
Fermat's Little Theorem: Theorem 7.36, p. 148.
Division with Remainder: Proposition 6.14, p. 126.