

**Primes and Divisibility:** If  $a/b$  is an integer, we say that  $b$  divides  $a$  or  $b$  is a factor or divisor of  $a$ . We also say this with the notation  $b|a$ , which you read “ $b$  divides  $a$ ”. Equivalently, there exists an integer  $m$  such that  $a = bm$ . A number  $n$  is **prime** if it has no divisors other than 1 and  $n$ . Otherwise  $n$  is called **composite**.

**Division Algorithm:** Let  $a$  and  $b$  be positive integers,  $b \geq a$ . Then there exist unique integers  $q, r$  satisfying  $q \geq 1$  and  $0 \leq r < a$  such that  $b = qa + r$ .

**GCD, LCM, Euclidean Algorithm:** Given positive integers  $a$  and  $b$ , there are integers  $s$  and  $t$  such that  $sa + tb = \gcd(a, b)$ . If there are integers  $s$  and  $t$  such that  $sa + tb = 1$ , then  $\gcd(a, b) = 1$ .

**Congruence:** Let  $m$  be a positive integer. If  $a - b$  is a multiple of  $m$ , we write  $a \equiv b \pmod{m}$ . For example,  $10 \equiv 1 \pmod{3}$ ,  $17 \equiv 102 \pmod{5}$ ,  $2 \equiv -1 \pmod{3}$ , and  $32 \equiv 0 \pmod{8}$ .

Facts:

- If you divide  $a$  by  $b$  and get a remainder of  $r$ , then  $a \equiv r \pmod{b}$ .
- There are only  $m$  “different” integers modulo  $m$ , since there are only  $m$  different remainders  $0, 1, 2, \dots, m - 1$ . We call these  $m$  numbers the **integers modulo  $m$**  or  $\mathbf{Z}_m$ .
- The statement  $a \equiv b \pmod{m}$  is equivalent to saying that there exists an integer  $k$  such that  $a = b + mk$ .
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$  and  $ac \equiv bd \pmod{m}$ .

The last statement is especially useful. For example, suppose we wanted to find the remainder when we divide  $2^{1000}$  by 17. Note that  $2^4 = 16 \equiv -1 \pmod{17}$ . Thus  $2^{1000} = (2^4)^{250} \equiv (-1)^{250} \equiv 1$ , so the remainder is 1.

A **Diophantine equation** is any equation whose variables only assume integral values. Given any Diophantine equation, there are four questions you should always ask:

- *Is the problem in “simple” form?* Always make sure that you have divided out all common factors, or assume the variables share no common factors, etc.
- *Do there exist solutions?* Sometimes you cannot actually solve the equation, but you can show that at least one solution exists.
- *Are there no solutions?* Quite frequently, this is the first question to ask. As with argument by contradiction, it is sometimes rather easy to prove that an equation has no solutions.
- *Can we find all solutions?* Once one solution is found, we try to understand how we can generate more solutions. It is sometimes quite tricky to prove that the solutions found are the complete set.

1. (Krantz 1.6.11) What is the last digit of  $3^{4798}$ ?
2. (Larson 3.2.3) What are the last two digits of  $3^{1234}$ ?
3. (Bicycle 82) If we multiply the four-digit number 1089 by 9 we get 9801, a four-digit number containing the same digits as the original number - only in reverse! We might say that 1089 is *reversed* by multiplication by 9. Is there a four-digit number that is reversed by multiplication by 4?
4. (Zeist) Find all solutions to the Diophantine equation  $x^2 + y^2 = 1000003$ .
5. (Larson 3.1.5) Prove that the fraction  $(21n+4)/(14n+3)$  is irreducible for every natural number  $n$ .
6. (Zeist) Show that if  $a^2 + b^2 = c^2$ , then  $3|ab$ .
7. Find all right triangles with integer sides such the area and perimeter are equal.