

## Page 24, Exercise 16, 20

### Exercise 16

**Determine  $7^{1000} \pmod{6}$ .**

Let  $a, b, k, n \in \mathbb{Z}$  such that  $k > 0$  and  $n > 0$ .

If  $a \equiv b \pmod{n}$ , then  $a^k \equiv b^k \pmod{n}$

Base Case:

$k = 1$

$a^1 \equiv b^1$  holds true

Inductive Step:

Suppose:  $a^k \equiv b^k \pmod{n}$

$a^{k+1} \equiv a^1 a^k$

$a^1 a^k \equiv a^1 b^k \pmod{n}$  by inductive hypothesis

$a^{k+1} \equiv b^k b \pmod{n}$  by base case

$a^{k+1} \equiv b^{k+1} \pmod{n}$

Thus,  $a^k \equiv b^k \pmod{n}$

Since  $7 \equiv 1 \pmod{6}$

$7^{1000} \equiv 1^{1000} \equiv 1 \pmod{6}$

**Determine  $6^{1001} \pmod{7}$ .**

$6^{1001} \pmod{7} \equiv 6 * 6^{1000} \pmod{7}$

$$\begin{aligned} 6^{1001} \pmod{7} &\equiv 6 * 6^{1000} \pmod{7} \\ &\equiv 6 * (6^2)^{500} \pmod{7} \\ &\equiv 6 * (36)^{500} \pmod{7} \\ &\equiv 6 * (1)^{500} \pmod{7} \\ &\equiv 6 \pmod{7} \end{aligned}$$

### Exercise 20

**Let  $p_1, p_2, \dots, p_n$ , be prime numbers. Show that  $p_1 * p_2 * \dots * p_n * p_{n+1}$  is not divisible by any of the  $n + 1$  primes.**

We will prove this by contradiction.

Suppose there are finitely many primes which are the ones listed.

Then, consider  $p_1 * p_2 * \dots * p_n * p_{n+1}$ .

This number is either composite or prime.

If it's prime, we just created a new prime, a contradiction.

If it's composite, that means it must be divisible by some prime.

By the Fundamental Theorem of Arithmetic,  $\exists t \in \mathbb{Z}$  such that

$p_1 t = q = p_1 * p_2 * \dots * p_n * p_{n+1}$ , which implies that  $p_i \mid 1$  for  $i \in \{1, 2, \dots, n\}$

This holds if and only if  $p_i = 1$ , a contradiction of the definition of a prime number.

Hence, there are infinitely many primes.