Modular Arithmetic II: Using Math to Send Passwords

BMC Int I Fall 2023

September 20, 2023

1 Last Week Review

Exercise 1.1. *What is the remainder when* 2^{304} *is divided by* 7*?*

Exercise 1.2. *What are the last two digits of* 3^{2004}*?*

Exercise 1.3. *What is the remainder when* $9 \times 99 \times 999 \times \cdots \times 99\cdots 9$ *is divided by* 1000*?*

2 Inverses

Theorem 2.1. *If* $(a, n) = 1$ *are relatively prime, then there exist* x, y *such that* $ax + ny = 1$*.*

Exercise 2.2. *Show that if* (a, n) *are relatively prime, then there is a number* $\frac{1}{a} \pmod{n}$ *so that* $a \cdot \frac{1}{a} \equiv 1 \pmod{n}$*.*

Exercise 2.3. *What is* $\frac{1}{3} \pmod{7}?\frac{1}{6} \pmod{25}$*?*

Exercise 2.4. *Prove that if* $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$ *is written as a fraction with* $p > 3$*, then* p^2 *divides the numerator.*

3 Combining Different Moduli

Theorem 3.1. *If* $n \equiv a_1 \pmod{m_1}, \ldots, n \equiv a_k \pmod{m_k}$ *with* $m_1, m_2, \ldots, m_k$ *all sharing no common factors, then we can combine these equivalences to* $n \equiv A \pmod{m_1 m_2 \ldots m_k}$*.*

Exercise 3.2. *Find* x *such that* $x \equiv 0 pmod 2$ *and* $x \equiv 0 \pmod{5}$*.*

Exercise 3.3. *Find all* x *such that* $x \equiv 3 \pmod{4}$ *and* $x \equiv 2 \pmod{7}$*.*

Exercise 3.4. *Find all* x *such that* $x \equiv 1 \pmod{3}$ *and* $x \equiv 0 \pmod{7}$*.*

Exercise 3.5. *Find all* x *such that* $x \equiv 1 \pmod{2}, x \equiv 2 \pmod{3}$*, and* $x \equiv 0 \pmod{5}$*.*

Exercise 3.6. *Find the smallest positive* x *such that* x *is a multiple of* 5*,* $x + 1$ *is a multiple of* 7*,* $x + 2$ *is a multiple of* 9*, and* $x + 3$ *is a multiple of* 11*.*

Exercise 3.7. *What are the last two digits of* 26^{2023}*?*

Exercise 3.8. *What are the last three digits of* 12^{101}*?*

4 RSA Encryption

Exercise 4.1. *Suppose that* p, q *are two prime numbers. Show that for any* a *relatively prime to* p, q *that* $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

Exercise 4.2. *In RSA encryption, the numbers* $N = pq$ *and* e *are told to everyone. To send a message* a*, send* $a^e \pmod{N}$*. Suppose that you receive the message* $m \pmod{N}$*, how to you decrypt it to get a back?*

Exercise 4.3. *Take* $p = 11, q = 17, e = 7$*. Then to send the secret number* 42*, what number do you send back? And how do you decrypt it?*