Problem Set 4

Name: SID:

Spring 2016 GSI:

1. Amaze Your Friends!

a. You want to trick your friends into thinking you can perform mental arithmetic with very large numbers What are the last digits of the following numbers?

i. 11^{2014}

Solution

ii. 9^{10001}

Solution

iii. $3^{987654321}$

Solution

b. You know that you can quickly tell a number n is divisible by 9 if and only if the sum of the digits of n is divisible by 9. Prove that you can use this trick to quickly calculate if a number is divisible by 9.

Solution

2. Short Answer: pmodular Arithmetic

a. What is the multiplicative inverse of 3 (mod 7)?

Solution

b. What is the multiplicative inverse of $n-1$ pmodulo n? (An expression that may involve n. Simplicity matters.)

Solution

c. What is the solution to the equation $3x = 6 \pmod 17$? (A number in $\{0, \ldots, 16\}$ or "No solution".)

Solution

d. Let $R_0 = 0; R_1 = 2; R_n = 4R_{n-1} - 3R_{n-2}$ for $n \geqslant 2$. Is $R_n = 2 \pmod 3$ for $n \geqslant 1$? (True or False)

Solution

e. Given that *extended* $-\gcd(53, m) = (1, 7, -1)$, that is $(7)(53) + (-1)m = 1$, what is the solution to $53x + 3 = 10 \pmod m$? (Answer should be an expression that is interpreted $\pmod m$, and shouldn't consist of fractions.)

Solution

3. Combining Moduli

Suppose we wish to work modulo $n = 40$. Note that $40 = 5 \times 8$, with $\gcd(5, 8) = 1$. We will show that in many ways working modulo 40 is the same as working modulo 5 and modulo 8, in the sense that instead of writing down $c \pmod{40}$, we can just write down $c \pmod{5}$ and $c \pmod{8}$.

a. What is $8 \pmod{5}$ and $8 \pmod{8}$? Find a number $a \pmod{40}$ such that $a \equiv 1 \pmod{5}$ and $a \equiv 0 \pmod{8}$.

Solution

b. Now find a number $b \pmod{40}$ such that $b \equiv 0 \pmod{5}$ and $b \equiv 1 \pmod{8}$.

Solution

c. Now suppose you wish to find a number $c \pmod{40}$ such that $c \equiv 2 \pmod{5}$ and $c \equiv 5 \pmod{8}$. Find c by expressing it in terms of a and b.

Solution

d. Repeat to find a number $d \pmod{40}$ such that $d \equiv 3 \pmod{5}$ and $d \equiv 4 \pmod{8}$.

Solution

e. Compute $c \times d \pmod{40}$. Is it true that $c \times d \equiv 2 \times 3 \pmod{5}$, and $c \times d \equiv 5 \times 4 \pmod{8}$?

Solution

4. The Last Digit

Let a be a positive integer. Consider the following sequence of numbers x defined by:

$$x_0 = a$$
$$x_n = x_{n-1}^2 + x_{n-1} + 1 \text{ if } n > 0$$

a. Show that if the last digit of a is 3 or 7, then for every n, the last digit of x_n is respectively 3 or 7.

Solution

b. Show that there exists $k > 0$ such that the last digit of x_n for $n \geqslant k$ is constant. Give the smallest possible k, *no matter what* a is.

Solution

5. Euclid's Extended GCD Algorithm

a. Compute the inerse of 37 modulo 64 using Euclid's extended GCD algorithm.

Solution

b. Prove that $\gcd(F_n, F_{n-1}) = 1$, where $F_0 = 0$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.

Solution

6. Bijections

Let n be an odd number. Let $f(x)$ be a function from $\{0, 1, \ldots, n-1\}$ to $\{0, 1, \ldots, n-1\}$. In each of these cases say whether or not $f(x)$ is a bijection. Justify your answer (either prove $f(x)$ is a bijection or give a counterexample).

a. $f(x) = 2x \pmod{n}$

Solution

b. $f(x) = 5x \pmod{n}$

Solution

c. n is prime and

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ x^{-1} \pmod{n} & \text{if } x \neq 0 \end{cases}$$

Solution

d. n is prime and $f(x) = x^2 \pmod{n}$.

Solution

7. Using RSA

Kevin and Bob decide to apply the RSA cryptography so that Kevin can send a secret message to Bob.

a. Assuming $p = 3, q = 11$, and $e = 7$, what is d? Calculate the exact value.

Solution

b. Following Part (a), what is the original message if Bob receives 4? Calculate the exact value.

Solution

8. Tweaking RSA

(This problem will not be graded, the solution will be posted on the problem thread on piazza.)

a. You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and p is prime. Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}, E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$. Show how you choose e and d in the encryption and decryption function, respectively. Prove that the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$

Solution

b. Can Eve now compute d in the decryption function? If so, by what algorithm?

Solution

c. Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where p, q, r are all prime). Explain how you can do so.

Solution