Name: KimJaeHwan
Student ID: 20230499

CSED261: Discrete Mathematics for Computer Science
Homework 5: Number Theory and Cryptography

Question 1. Show that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where a, b, c, d, and m are integers with $m \geq 2$, then $a - c \equiv b - d \pmod{m}$.

Solutions

If $a \equiv b \pmod{m}$, then $a = b + km$ for some integer k. Similarly, if $c \equiv d \pmod{m}$, then $c = d + lm$ for some integer l. Therefore, $a - c = b + km - d - lm = (b - d) + m(k - l)$, so $a - c \equiv b - d \pmod{m}$.

Question 2. Show that a positive integer is divisible by 11 if and only if the difference of the sum of its decimal digits in even-numbered positions and the sum of its decimal digits in odd-numbered positions is divisible by 11.

Solutions

First, let's think about the properties of the number 11. We can make 99 using 11, Similary, 9999, 999999 is possible. This means, one digit number $a \equiv a \pmod{11}$, then two digits number $10 \times b \equiv -b \pmod{11}$ by 11, because of $10 \equiv -1 \pmod{11}$. three digits number $100 \times c \equiv c \pmod{11}$ by 99, because of $100 = 11 \times 9 + 1 \equiv 1 \pmod{11}$. This property can be applied to any number.

In conclusion, even-numbered positions, $a \times 10^{2n-1} \equiv a \pmod{11}$ because of $10^{2n-1} \equiv 1 \pmod{11}$, and odd-numbered positions, $b \times 10^{2n} \equiv -b \pmod{11}$, because of $10^{2n} \equiv -1 \pmod{11}$

Finally, we can get, if the difference of the sum of its decimal digits in even-numbered positions and the sum of its decimal digits in odd-numbered positions is divisible by 11,

$$\begin{aligned} N &= a_0 \times 1 + a_1 \times 10 + a_2 \times 100 + \cdots + a_n \times 10^n \\ &\equiv a_0 - a_1 + a_2 - a_3 + \cdots \pm a_n \pmod{11} \\ &\equiv 0 \pmod{11} \end{aligned}$$

So, N is divisible by 11.

Question 3. Use the Euclidean algorithm to find

(a) gcd(1, 5)

(b) gcd(100, 101)

(c) gcd(123, 277)

(d) gcd(1529, 14039)

(e) gcd(1529, 14038)

(f) gcd(11111, 111111)

Solutions

(a) $5 = 5 \times 1 + 0$, $\gcd(1, 5) = 1$

(b) $101 = 100 \times 1 + 1$, $\gcd(100, 101) = \gcd(1, 100)$
$100 = 1 \times 100 + 0$, $\gcd(1, 100) = 1$

(c) $277 = 123 \times 2 + 31$, $\gcd(123, 277) = \gcd(31, 123)$
$123 = 31 \times 3 + 30$, $\gcd(31, 123) = \gcd(30, 31)$
$31 = 30 \times 1 + 1$, $\gcd(30, 31) = \gcd(1, 30)$
$30 = 1 \times 30 + 0$, $\gcd(1, 30) = 1$

(d) $14039 = 1529 \times 9 + 278$, $\gcd(1529, 14039) = \gcd(278, 1529)$
$1529 = 278 \times 5 + 139$, $\gcd(278, 1529) = \gcd(139, 278)$
$278 = 139 \times 2 + 0$, $\gcd(139, 278) = 139$

(e) $14038 = 1529 \times 9 + 277$, $\gcd(1529, 14038) = \gcd(277, 1529)$
$1529 = 277 \times 5 + 144$, $\gcd(277, 1529) = \gcd(144, 277)$
$277 = 144 \times 1 + 133$, $\gcd(144, 277) = \gcd(133, 144)$
$144 = 133 \times 1 + 11$, $\gcd(133, 144) = \gcd(11, 133)$
$133 = 11 \times 12 + 1$, $\gcd(11, 133) = \gcd(1, 11)$
$11 = 1 \times 11 + 0$, $\gcd(1, 11) = 1$

(f) $111111 = 11111 \times 10 + 1$, $\gcd(11111, 111111) = \gcd(1, 11111)$
$11111 = 1 \times 11111 + 0$, $\gcd(1, 11111) = 1$

Question 4. Show that if a, b, and m are integers such that $m \geq 2$ and $a \equiv b \pmod{m}$, then $\gcd(a,m) = \gcd(b,m)$.

Solutions

$a \equiv b \pmod{m}$, then we can represent $a = b + km$ for some integer k. Let $x = \gcd(a, m)$ and $y = \gcd(b, m)$. Then x divides both a and m because x is gcd of them. Then, x can also divide $b = a - km$ because x can divide a and m. Therefore, x divides y because y is gcd of b and m and x can divide both. Similary, y divides a and m because y is gcd of b and m. Then, y can also divide $a = b + km$ because y can divide b and m. Therefore, y divides x because x is gcd of a and m and y can divide both. So, x can divide y and vice versa. This means $x = y$ and $\gcd(a, m) = \gcd(b, m)$.

Question 5. Solve the system of congruence $x \equiv 3 \pmod 6$ and $x \equiv 4 \pmod 7$ using the method of back substitution.

Solutions

$x \equiv 3 \pmod 6$ implies $x = 3 + 6k$ for some integer k. Substitute this into the second congruence: $3 + 6k \equiv 4 \pmod 7$. Solving this congruence, we get $6k \equiv 1 \pmod 7$, then k is the inverse of 6 modulo 7. Because of gcd(6, 7) = 1, we can use the Bezout's theorem to find the inverse. Using the Euclidean algorithm, we have: $7 = 6 \times 1 + 1$, $-1 \times 6 + 1 \times 7 = 1$, so the inverse of 6 modulo 7 is -1. Finally, some integer $k = 7m - 1$ for some integer m. Then, $x = 3 + 6(7m - 1) = 42m - 3$. So $x \equiv -3 \equiv 39 \pmod{42}$.

Question 6. Suppose that the ciphertext DVE CFMV KF NFEUVI, REU KYRK ZJ KYV JVVU FW JTZVETV was produced by encrypting a plaintext message using a shift cipher. What is the original plaintext?

Solutions

For decrypting shift cipher, we need to find the key using relative frequences of letters 'E' or 'T'. In encrypted text "DVE CFMV KF NFEUVI, REU KYRK ZJ KYV JVVU FW JTZVETV", the most frequent letter is 'V'. Let's assume that 'V' is encypted is 'E' in plaintext, then key of decryption function $f^{-1}(x) = (p - k) \pmod{26}$ is $k = 17$. So,

Encrypt	Decrypt
A $\to$ R	A $\to$ J
B $\to$ S	B $\to$ K
C $\to$ T	C $\to$ L
D $\to$ U	D $\to$ M
E $\to$ V	E $\to$ N
F $\to$ W	F $\to$ O
G $\to$ X	G $\to$ P
H $\to$ Y	H $\to$ Q
I $\to$ Z	I $\to$ R
J $\to$ A	J $\to$ S
$\vdots$	$\vdots$

Then, the plain text is,
MEN LOVE TO WONDER, AND THAT IS THE SEED OF SCIENCE.