Ehren Schindelar
RIN 661677600
Oct. 9, 2018

1

a) The equation $a \equiv b \pmod{n}$, is equivalent to the equation $(a \mod n) = (b \mod n)$. Due to the commutative nature of the equals sign, it is easy to say that $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.

b) The equation $(a \mod n) = (b \mod n)$ can be represented by $a + k * n = b + l * n$ for some integral constants k and l.

$$a + k * n = b + l * n$$

By applying this to the other equation using two new constants o and p, our original two equations can be expressed as:

$$a + k * n = b + l * n \text{ and } b + o * n = c + p * n$$

We add the two equations together and get:

$$a + b + k * n + o * n = b + c + l * n + p * n$$
$$a + (k + o) * n = c + (l + p) * n$$

Since $(k + o)$ and $(l + p)$ are both integral constants, we can express the equation as $(b \mod n) = (c \mod n)$, which is equivalent to $b \equiv c \pmod{n}$.

Ehren Schindelar
RIN 661677600
Oct. 9, 2018

2

a) 1234 mod 4321

$$4321 = 3 * 1234 + 619$$
$$1234 = 619 + 615$$
$$619 = 615 + 4$$
$$615 = 153 * 4 + 3$$
$$4 = 3 + 1$$
$$619 = 4321 - 3 * 1234$$
$$615 = 1234 - 619 = 1234 - (4321 - 3 * 1234) = 4 * 1234 - 4321$$
$$4 = 619 - 615 = 4321 - 3 * 1234 - (4 * 1234 - 4321) = 2 * 4321 - 7 * 1234$$
$$3 = 615 - 153 * 4 = 4 * 1234 - 4321 - 153 * (2 * 4321 - 7 * 1234) = 1075 * 1234 - 307 * 4321$$
$$1 = 4 - 3 = 2 * 4321 - 7 * 1234 - (1075 * 1234 - 307 * 4321) = 309 * 4321 - 1082 * 1234$$

The multiplicative inverse of 1234 mod 4321 is -1082, which is equivalent to 3239 mod 4321

b)24140 mod 40902

$$40902 = 24140 + 16762$$
$$24140 = 16762 + 7378$$
$$16762 = 2 * 7378 + 2006$$
$$7378 = 3 * 2006 + 1360$$
$$2006 = 1360 + 646$$
$$1360 = 2 * 646 + 68$$
$$646 = 9 * 68 + 34$$
$$68 = 2 * 34$$

$gcd(24140, 40902) = 34 \neq 1$, therefore a multiplicative inverse does not exist.

c)550 mod 1769

$$1769 = 3 * 550 + 119$$
$$550 = 4 * 119 + 74$$
$$119 = 74 + 45$$
$$74 = 45 + 29$$
$$45 = 29 + 16$$
$$29 = 16 + 13$$
$$16 = 13 + 3$$
$$13 = 4 * 3 + 1$$
$$119 = 1769 - 3 * 550$$
$$74 = 550 - 4 * 119 = 13 * 550 - 4 * 1769$$
$$45 = 119 - 74 = 5 * 1769 - 16 * 550$$

$$
\begin{gathered}
29 = 74 - 45 = 29 * 550 - 9 * 1769 \\
16 = 45 - 29 = 14 * 1769 - 45 * 550 \\
13 = 29 - 16 = 74 * 550 - 23 * 1769 \\
3 = 16 - 13 = 37 * 1769 - 119 * 550 \\
1 = 13 - 4 * 3 = 550 * 550 - 171 * 1769
\end{gathered}
$$

The multiplicative inverse of $550 \mod 1769$ is 550.

Ehren Schindelar
RIN 661677600
Oct. 9, 2018

3

a) $x^3 + 1$
This is reducible over $GF(2)$.
One factor is $x + 1 = (x^3 + 1)/(x^2 - x + 1)$

b) $x^3 + x^2 + 1$
This is obviously not reducible, as it's value is always $1 \mod 2$.

c) $x^4 + 1$
This is reducible over $GF(2)$
One factor is $(x^2 + x - 1) * (x^2 - x - 1) = x^4 - 2x^2 + 1 \equiv x^4 + 1$ over $GF(2)$

Ehren Schindelar
RIN 661677600
Oct. 9, 2018

4

a) $x^3 - x + 1$ and $x^2 + 1$ over $GF(2)$
All of the coefficients can be modulo 2 in the following equations.

$$x^3 - x + 1 \equiv x^3 + x + 1 \text{ in } GF(2)$$
$$x^3 - x + 1 = x * (x^2 + 1) - 2x + 1 \equiv x * (x^2 + 1) + 1 \; GF(2)$$

These two are relatively prime.

b) $x^5 + x^4 + x^3 - x^2 - x + 1$ and $x^3 + x^2 + x + 1$ over $GF(3)$
All of the coefficients can be modulo 3 in the following equations.

$$x^5+x^4+x^3-x^2-x+1 = (x^2)*(x^3+x^2+x+1)-2x^2-x+1 = x^2*(x^3+x^2+x+1)+x^2-x+1$$
$$x^3 + x^2 + x + 1 = (x + 2) * (x^2 - x + 1) + 2x - 1$$
$$x^2 - x + 1 = (2x) * (2x + 2) + x + 1$$
$$2x + 2 = 2 * (x + 1)$$

The GCD of $x^5 + x^4 + x^3 - x^2 - x + 1$ and $x^3 + x^2 + x + 1$ over $GF(3)$ is $x + 1$.

5

Ehren Schindelar
RIN 661677600
Oct. 9, 2018

5

We know that $H(K|C) = H(K) + H(P) - H(C)$, so compute $H(K)$, $H(P)$, and $H(C)$. Using $H(X) = \sum_i^n p_i \log_2 p_i$, $H(K) = H(P) \approx -0.4515$

To compute $H(C)$, we neet compute all p_i, which can be done by simming the probabilities of all corresponding $E_{k_i}(j)$ e.g., $p_1 = p(e_{k_1}(a)) + p(e_{k_1}(c)) + p(e_{k_2}(c)). = p(a) * p(k_1) + p(c) * p(k_1) + p(c) * p(k_2)$ since the plaintext and key are independant. As such, $p_1 = 0.5$, $p_2 = 0.25$, $p_3 = 0.125$, and $p_4 = 0.125$. Now we can compute $H(C) \approx -.5268$

Therefore, $H(K|C) \approx -0.3762$