Homework Assignment 5 - Introduction To Cryptography

Ton That Tam Dinh

October 28, 2017

Problem DSDC-2.

Proof. 0) Firstly we test the this operation is close. If we have $x, y \in Z$then $x * y \in Z$.
1) Identity Law: We have $e = 0 \in Z$ such that e*x = x = x*e.
2) Inverse Law: For every $a \in Z$ there is a $a^{-1} \in Z$. If a is odd number we have $a^{-1} = a$. Because $a * a{-}1 = a - a = 0$ If a is even number we have $a^{-1} = -a$. Because $a * a^{-1} = a + -a = 0$
3) When a and b are even numbers we have: (a*b)*c = (a + b) + c = a*(b+c) = a + (b + c)
if both a and b are odd numbers we have: (a*b)*c = (a - b) + c = a - (b - c) = a*(b*c)
when a is even and b is odd we have: (a*b)*c = (a + b) - c = a + (b - c) = a*(b*c)
when a is odd and b is even we have: (a*b)*c = (a - b) - c = a - (b + c) = a*(b*c). So for all $a, b, c \in Z$ we have (a*b)*c = a*(b*c). It means operaton * sastify Commutative Law. Finnally, we have (Z, *) is a group. □

Problem DSDC-3.

Proof. 3a) With x = -1, we can't find y = x^{-1} in Q so (Q, *) is not a group.
3b) Let's define Q1 = Q - {1}
0) If $x, y \in Q1$ so $x + y + xy \in Q1$ it means this operation is close in Q1.
1) We have $e = 0 \in Q1$ sastify that $x * e = e * x = x + e + x * e = x$, so this operation sastifies Identity Law.
2) For each $x \in Q1$ 1 there is exist $y = \frac{-x}{x+1} \in Q1$ such that x * y = x + y + xy = x + y(x + 1) = 0 = e. It means this operation sastifies Inverse Law.
3) For all $x, y, z \in Q1$ we have (x*y)*z = (x+y+xy)*z = (x+y+xy) + z + (x+y+xy)z = x + y + xy + z + xz + yz + xyz x*(y*z) = x + (y*z) + x(y*z) = x + y + z + yz + x(y + z + yz) = x + y + z + yz + xy + xz + xyz = (x*y)*z So this operaton sastifies the Communative Law. Finally, (Q1, *) is a group. □

Problem DSDC-14.

Proof. Let's define $6Z = \{\ 6 * x \mid x \in Z\}$ and $15Z = \{\ 15 * y \mid y \in Z\}$. So $6Z \cap 15Z = \{\ gcd(6, 15) * y \mid y \in Z\} = \{\ 3 * y \mid y \in Z\}$ so 3 is a generator of $6Z \cap 15Z$.

□

Problem 1.32.

Proof. (a) 2 is primitive root modulo p when p = 7 and p = 13.
(b) 3 is primitive root modulo p when p = 5 and p = 7.
(c) (i) g = 5,
(ii) g = 2,
(iii) g = 6,
(iv) g = 3
(d) There are 4 primitive roots modulo 11.All of them are: 2, 6, 7, 8. The number of primitive roots modulo 11 equal to $\phi(10)$

$\square$

Problem 31.

Proof. Firstly we easily test that (C - {1}, *) is the group and $G \subset C-\{1\}$. And then if we want to proof $G = \{\ m + n * i | m, nQ, i^2 = 1\} - \{\ 0\}$ we just test that:
(i) if $x, y \in G$ then $xy \in G$
(ii) if $x \in G$ then $x^{-1} \in G$

Firstly, we will test the (i) condition. When $x, y \in G$ it means $x = m_1 + n_1 i$ and $y = m_2 + n_2 i$ so $x * y = m_1 * m_2 - n_1 * n_2 + (m_1 n_2 + m_2 n_1)i$. Since $m_1, m_2, n_1, n_2 \in Q$ so $m_1 * m_2 - n_1 * n_2 \in Q$ and $m_1 n_2 + m_2 n_1 \in Q$. It proves that $x * y \in G$
In the next step, we will test the second condition. With $x \in G$, we easily find that $x^{-1} = \frac{m-ni}{m^2-n^2}$. Since $m, n \in Q$ so that $\frac{m}{m^2-n^2} and \frac{-n}{m^2-n^2} \in Q$. It means $x^{-1} \in G$ $\square$