

HOMWORK 4

1. Show that the gcd operation is associative. That is: $gcd(a, gcd(b, c)) = gcd(gcd(a, b), c)$.
2. Compute the values (d, x, y) generated by the extended Euclidean Algorithm (899,493). (Exercise 33.2-2)
3. Draw the group operation tables for $(\mathbf{Z}_4, +_4)$ and $(\mathbf{Z}^*_5, *_5)$. Show that these groups are isomorphic by exhibiting a 1—1 correspondence $alpha(.)$ between their elements such that $a+b$ is congruent to c in modulus n ($a+b=c \pmod n$) if and only if $alpha(a)*alpha(b)=alpha(c) \pmod 5$. (33.3-1)
4. List all subgroups of \mathbf{Z}_9 and \mathbf{Z}^*_13 .
5. Draw a table showing the order of every element in \mathbf{Z}^*_11 . Pick the smallest primitive root g and compute a table giving $discrete-log_{(11,g)}(x)$ for all x in \mathbf{Z}^*_11 . (33.6-1)
6. The question posted on the board during the second class of Public Key Cryptography.