CS 6101 MFCS Test-III, Sept. 2017. Name:

1. Let a, b be two two integers. Consider the set $S(a,b)$ of all elements of the form $\alpha a + \beta b$, where α, β are integers. Which of the following is true? Justify your answer. 1) $S(a,b)$ a cyclic group w.r.t addition 2) $S(a,b)$ is not a cyclic group w.r.t addition, but is a group 3) $S(a,b)$ is not a group w.r.t addition. $\boxed{3}$

   Soln: $S(a,b)$ is a cyclic group with respect to addtion. Let $d = GCD(a,b)$. By definition, every element $x \in S(a,b)$ must be of the form $x = \alpha a + \beta b$. Thus, x must be a multiple of d (why?). Moreover, by Euclid's algorithm, there exists $\alpha_0, \beta_0 \in \mathbf{Z}$ such that $d = \alpha_0 a + \beta_0 b$. Hence $d \in S(a,b)$ and elements of $S(a,b)$ are precisely multiples of d. Thus d must be a generator of $S(a,b)$.

2. In $\mathbf{Z}_{20}^*$, consider the subgroup $H = \{1, 11\}$. Write down all the cosets of this group. $\boxed{3}$

   Soln: $\mathbf{Z}_{20}^* = \{1,3,7,11,13,17,19\}$. Cosets are $1H = \{1,11\}, 3H = \{3,13\}, 7H = \{7,17\}, 9H = \{9,19\}$.

3. Let $(G, ., 1)$ be any group (not necessarily Abelian) and let H a subgroup of G. Define the following relation in G: For any $a, b \in G$, aRb if $ab^{-1} \in H$. Is R an equivalance relation? (Prove/Provide counter-example). $\boxed{3}$

   Soln: R is an equivalance relation. For every $a \in G$, $aa^{-1} = 1 \in H$. Hence aRa. For $a, b \in G$, If aRb, then $ba^{-1} = (ab^{-1})^{-1} \in H$. Hence bRa. Finally, if aRb and bRc for some $a, b, c \in G$, then $ac^{-1} = ab^{-1}bc^{-1} \in H$. Hence aRc.

4. Complete the following version of the Euclid's algorithm that on input positive integers a, b returns a tripple (d, x, y) where $d =$GCD(a,b) and x, y are integers satisfying $xa + yb = d$. Derive the computation of the return values of each recursive call. $\boxed{3}$

```
(d,x,y)euclid(a,b) {
         if (a==b) return(b,0,1);  // other correct possibilites also.
         if (b>a) {
                (d,x,y) = euclid(b,a); return (d,y,x);
         } else {
                (d,x,y) = euclid(a-b,b); return (d,x,y-x);
         }
}
```

5. Let G be a cyclic group of order n generated by $a \in G$. Let d divide n. Suppose an element a^t has order $\frac{n}{d}$, show that t is a multiple of d. $\boxed{3}$

   Soln: $(a^t)^{\frac{n}{d}} = 1 \Rightarrow a^{\frac{tn}{d}} = 1$. Hence $o(a) | \frac{tn}{d}$ (Lagrange) $\Rightarrow n | \frac{tn}{d} \Rightarrow 1 | \frac{t}{d} \Rightarrow \frac{t}{d}$ is an integer.