

1. Find all elements of groups  $\mathbb{Z}_7$ ,  $\mathbb{Z}_7^*$ ,  $\mathbb{Z}_8$ ,  $\mathbb{Z}_8^*$ .
2. Using Euclidean Algorithm find the inverse of 7 in  $\mathbb{Z}_{31}^*$  and  $\mathbb{Z}_{137}^*$ .
3. Find the smallest generator of the group  $\mathbb{Z}_{31}^*$ .
4. Find all subgroups of  $\mathbb{Z}_6$ .
5. Find all subgroups of  $\mathbb{Z}_8^*$ .
6. Is  $\mathbb{Z}_2$  a subgroup of  $\mathbb{Z}_4$ ?
7. Is 3 a generator of  $\mathbb{Z}_{53}^*$ ?
8. Is the group  $(\mathbb{Z}, \circ)$  cyclic, if  $a \circ b = a + b - 5$ . If yes, find the generators.
9. Which group is cyclic:  $\mathbb{Z}_5^*$ ,  $\mathbb{Z}_8^*$ ,  $\mathbb{Z}_{15}^*$ ?
10. For all  $a \in \mathbb{Z}_9^*$  find  $\langle a \rangle$  and  $|a|$ . Is  $\mathbb{Z}_9^*$  cyclic?
11. For all  $a \in \mathbb{Z}_{14}^*$  find  $\langle a \rangle$  and  $|a|$ . Is  $\mathbb{Z}_{14}^*$  cyclic?
12. Prove, that  $5n + 3$  and  $7n + 4$  are relatively prime for any positive  $n$ .
13. Find primes  $p, q$  if  $n = p \cdot q = 414847$  and  $\phi(n) = 413280$ .
14. Find an integer  $a$  such that  $a \equiv 4 \pmod{6}$  and  $a \equiv 5 \pmod{35}$ .
15. Find an integer  $a$  such that  $a \equiv 4 \pmod{7}$  and  $a \equiv 1 \pmod{19}$ .
16. Find an integer  $a$  such that  $a \equiv 38 \pmod{103}$  and  $a \equiv 81 \pmod{83}$ .
17. Find an integer  $a$  such that  $a \equiv 4 \pmod{6}$  and  $a \equiv 5 \pmod{35}$ .
18. Find an integer  $a$  such that  $a \equiv 4 \pmod{7}$  and  $a \equiv 1 \pmod{19}$ .
19. Find an integer  $a$  such that  $a \equiv 38 \pmod{91}$ ,  $a \equiv 81 \pmod{83}$  and  $a \equiv 3 \pmod{95}$ .
- 20.
21. Knowing  $n = 5133$  and

0	1	2	3	4	5	6	7	8	9
RY	SYS	TEM	O	TY	MA	GA	EK	WA	TE

encrypt the message SYSTEM, THEORY using Rabin method.

22. Using Rabin method decrypte the messege  $E(M) = 17(\text{mod } 1121)$ , if you know that  $1121 = 19 \cdot 59$ .

0	1	2	3	4	5	6	7	8	9
A	M	L	D	F	T	Y	O	Z	K

23. Knowing that  $n = 589 = 19 \cdot 31$ ,  $e = 53$  and encrypting function for RSA cryptosystem is  $E(M) = M^e(\text{mod } n)$  find decrypting function (for RSA method).
24. Knowing that  $n = 589 = 19 \cdot 31$ ,  $d = 23$  and decrypting function for RSA cryptosystem is  $D(N) = N^d(\text{mod } n)$  find encrypting function (for RSA method).
25. Let *day-23, nice-7, good-1, have-4, luck-3, the-59, always-54, reason-47*. Using RSA method for  $p = 11$ ,  $q = 13$ ,  $e = 11$  decrypt the message "113,1".