**“TASDIQLAYMAN”**

**“Kriptologiya” kafedrasi   
mudiri Xudoykulov Z.T.**

**\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_ 2024-yil**

**Kriptografiya 1 fani bo‘yicha yakuniy nazorat savollari**

1. Evklid va kengaytirilgan Evklid algoritmi qoidasi hamda ularga doir misollar.
2. hamda sonlarining eng katta umumiy bo‘luvchisini Evklid algoritmi olrqali toping.
3. hamda sonlarining eng katta umumiy bo‘luvchisini Evklid algoritmi olrqali toping.
4. hamda sonlarining eng katta umumiy bo‘luvchisini Evklid algoritmi olrqali toping.
5. sonini maydonda teskarisini toping.
6. va sonlarini maydonda ko‘paytmasini toping.
7. sonini maydonda teskarisini toping.
8. va sonlarini maydonda ko‘paytmasini toping.
9. sonini maydonda teskarisini toping.
10. va sonlarini maydonda ko‘paytmasini toping.
11. Modulyar arifmetika va uning xossalarini tushintirib bering.
12. Chiziqli mosliklar va ularning xossalari. Chiziqli mosliklarni yechimi mavjudligini tekshirish hamda yechimlar sonini aniqlash qoidalarini tushintiring.
13. chiziqli moslikni yeching.
14. chiziqli moslikni yeching.
15. chiziqli moslikni yeching.
16. Chiziqli diafant tenglamalarini yechish.
17. chiziqli diafant tenglamasini yeching.
18. chiziqli diafant tenglamasini yeching.
19. chiziqli diafant tenglamasini yeching.
20. Katta darajali sonlarni modul bo‘yicha qoldig‘ini topishning effektiv usuli qoidasini tushintiring.
21. sonini qiymatini hisoblang.
22. sonini qiymatini hisoblang.
23. sonini qiymatini hisoblang
24. Eyler funksiyasi va undan kelib chiqadigan teoremalarni tushintiring.
25. Birlamchi ildiz tushunchasi, berilgan modul bo‘yicha birlamchi ildizlar sonini va qiymatlarini hisoblash qoidasini tushintiring.
26. Biror soni berilgan modul bo‘yicha tartibini topish qoidasini tushintiring.
27. sonining modul bo‘yicha tartibini hisoblang.
28. sonining modul bo‘yicha tartibini hisoblang.
29. sonining modul bo‘yicha tartibini hisoblang.
30. sonining Eyler funksiyasi qiymatini hisoblang.
31. sonining Eyler funksiyasi qiymatini hisoblang.
32. sonining Eyler funksiyasi qiymatini hisoblang.
33. sonini birlamchi ildizlar sonini va qiymatlarini toping.
34. sonini birlamchi ildizlar sonini va qiymatlarini toping.
35. sonini birlamchi ildizlar sonini va qiymatlarini toping.
36. Qoldiqlar haqidagi Xitoy teoremasi.
37. va ushbu chiziqli mosliklari qoldiqlar haqida Xitoy teoremasi orqali hisoblang.
38. va ushbu chiziqli mosliklari qoldiqlar haqida Xitoy teoremasi orqali hisoblang.
39. , , va ushbu chiziqli mosliklari qoldiqlar haqida Xitoy teoremasi orqali hisoblang.
40. Parametrli algebra asosida amallarni bajarish (sonlarni ko‘paytirish, darajaga oshirish va mdul bo‘yicha teskarisini topish).
41. va sonini modul bo‘lganda, parametr bo‘yicha ko‘paytiring.
42. va sonini modul bo‘lganda, parametr bo‘yicha ko‘paytiring.
43. va sonini modul bo‘lganda, parametr bo‘yicha ko‘paytiring.
44. sonini modul bo‘lganda, parametr bo‘yicha darajaga oshiring.
45. sonini modul bo‘lganda, parametr bo‘yicha darajaga oshiring.
46. sonini modul bo‘lganda, parametr bo‘yicha darajaga oshiring.
47. sonini modul bo‘lganda, parametr bo‘yicha teskarisini toping.
48. sonini modul bo‘lganda, parametr bo‘yicha teskarisini toping.
49. sonini modul bo‘lganda, parametr bo‘yicha teskarisini toping.
50. kvadrat mosliklarni yechish qoidasini tushintiring.
51. kvadrat moslikni yeching.
52. kvadrat moslikni yeching.
53. kvadrat moslikni yeching.
54. Berilgan to‘plam guruh bo‘lishi uchun qanday shartlar bajarilishi shart.
55. Berilgan to‘plam xalqa bo‘lishi uchun qanday shartlar bajarilishi shart.
56. Berilgan to‘plam maydom bo‘lishi uchun qanday shartlar bajarilishi shart.
57. Lejandr simvoli va uning xossalarini tushintirib bering.
58. Lejandr simvolini Gauss Lemmasi – teoremasi orqali hisoblash usuli.
59. modul bo‘yicha kavadrat chegirma bo‘ladigan barcha qiymatlarni Gauss Lemmasi orqali hisoblash qoidasini tushintiring.
60. modul bo‘yicha kavadrat chegirma bo‘ladigan barcha qiymatlarni Gauss Lemmasi orqali hisoblang.
61. modul bo‘yicha kavadrat chegirma bo‘ladigan barcha qiymatlarni Gauss Lemmasi orqali hisoblang.
62. Lejandr simvolini Eyler kriteriyasi orqali hisoblash qoidasini tushintiring.
63. modul bo‘yicha kavadrat chegirma bo‘ladigan barcha qiymatlarni Eyler kriteriyasi orqali hisoblang.
64. modul bo‘yicha kavadrat chegirma bo‘ladigan barcha qiymatlarni Eyler kriteriyasi orqali hisoblang.
65. modul bo‘yicha kavadrat chegirma bo‘ladigan barcha qiymatlarni Eyler kriteriyasi orqali hisoblang.
66. Lejandr simvolini birlamchi ildiz orqali hisoblash qoidasini tushintiring.
67. modul bo‘yicha kavadrat chegirma bo‘ladigan barcha qiymatlarni birlamchi ildiz qiymati orqali hisoblang.
68. modul bo‘yicha kavadrat chegirma bo‘ladigan barcha qiymatlarni hisoblang.
69. modul bo‘yicha kavadrat chegirma bo‘ladigan barcha qiymatlarni hisoblang.
70. Lejandr simvoli qiymatini toping.
71. Lejandr simvoli qiymatini toping.
72. Lejandr simvoli qiymatini toping.
73. Sonlarni faktorlarga ajratishning Ferma usuli qoidasini tushintiring.
74. sonini Ferma usuli orqali faktorlarga ajrating.
75. sonini Ferma usuli orqali faktorlarga ajrating.
76. sonini Ferma usuli orqali faktorlarga ajrating.
77. Sonlarni faktorlarga ajratishning Pollard usuli qoidasini tushintiring.
78. sonini Pollard usuli orqali faktorlarga ajrating.
79. sonini Pollard usuli orqali faktorlarga ajrating.
80. sonini sonini Pollard usuli orqali faktorlarga ajrating.
81. Sonlarni tublikka sinashning Ferma testi qoidasini tushintiring.
82. sonini Ferma testi orqali kamida 3 ta guvoh asosida tublikka tekshiring.
83. sonini Ferma testi orqali kamida 3 ta guvoh asosida tublikka tekshiring.
84. sonini Ferma testi orqali kamida 3 ta guvoh asosida tublikka tekshiring.
85. Sonlarni tublikka sinashning Solavey-Shtrassen testi qoidasini tushintiring.
86. sonini Solavey-Shtrassen testi orqali kamida 3 ta guvoh asosida tublikka tekshiring.
87. sonini Solavey-Shtrassen testi orqali kamida 3 ta guvoh asosida tublikka tekshiring.
88. sonini Solavey-Shtrassen testi orqali kamida 3 ta guvoh asosida tublikka tekshiring.
89. Sonlarni tublikka sinashning Rabin-Miller testi qoidasini tushintiring.
90. sonini Rabin-Miller testi orqali kamida 3 ta guvoh asosida tublikka tekshiring.
91. sonini Rabin-Miller testi orqali kamida 3 ta guvoh asosida tublikka tekshiring.
92. sonini Rabin-Miller testi orqali kamida 3 ta guvoh asosida tublikka tekshiring.
93. Polig-Hellman diskret logarifmlash usuli qoidasini tushintiring.
94. ifodadan qiymatini hisoblang.
95. ifodadan qiymatini hisoblang.
96. ifodadan qiymatini hisoblang.
97. Elliptik egri chiziqda nuqtalarni qo‘shish hamda ikkilantirishning geometric ma’nosini tushintirib bering.
98. , . va ni hisoblang, bunda .
99. , . va ni hisoblang, bunda .
100. , . va ni hisoblang, bunda .

**Tuzuvchi:**

**“Kriptologiya” kafedrasi katta o‘qituvchisi Mardiyev U.R.**