通过如下代码计算质数的原根。



求出211的原根

211的原根有：

[2, 3, 7, 17, 22, 29, 35, 39, 41, 48, 57, 72, 75, 85, 91, 92, 106, 108, 112, 116, 118, 127, 130, 131, 133, 141, 142, 145, 149, 152, 155, 158, 159, 160, 162, 164, 165, 166, 167, 174, 175, 181, 187, 191, 195, 202, 205, 207]

测试211的原根112（即p=211 g=112）

112^1 mod 211 = 112

112^2 mod 211 = 95

112^3 mod 211 = 90

112^4 mod 211 = 163

112^5 mod 211 = 110

112^6 mod 211 = 82

112^7 mod 211 = 111

112^8 mod 211 = 194

112^9 mod 211 = 206

112^10 mod 211 = 73

112^11 mod 211 = 158

112^12 mod 211 = 183

112^13 mod 211 = 29

112^14 mod 211 = 83

112^15 mod 211 = 12

112^16 mod 211 = 78

112^17 mod 211 = 85

112^18 mod 211 = 25

112^19 mod 211 = 57

112^20 mod 211 = 54

112^21 mod 211 = 140

112^22 mod 211 = 66

112^23 mod 211 = 7

112^24 mod 211 = 151

112^25 mod 211 = 32

112^26 mod 211 = 208

112^27 mod 211 = 86

112^28 mod 211 = 137

112^29 mod 211 = 152

112^30 mod 211 = 144

112^31 mod 211 = 92

112^32 mod 211 = 176

112^33 mod 211 = 89

112^34 mod 211 = 51

112^35 mod 211 = 15

112^36 mod 211 = 203

112^37 mod 211 = 159

112^38 mod 211 = 84

112^39 mod 211 = 124

112^40 mod 211 = 173

112^41 mod 211 = 175

112^42 mod 211 = 188

112^43 mod 211 = 167

112^44 mod 211 = 136

112^45 mod 211 = 40

112^46 mod 211 = 49

112^47 mod 211 = 2

112^48 mod 211 = 13

112^49 mod 211 = 190

112^50 mod 211 = 180

112^51 mod 211 = 115

112^52 mod 211 = 9

112^53 mod 211 = 164

112^54 mod 211 = 11

112^55 mod 211 = 177

112^56 mod 211 = 201

112^57 mod 211 = 146

112^58 mod 211 = 105

112^59 mod 211 = 155

112^60 mod 211 = 58

112^61 mod 211 = 166

112^62 mod 211 = 24

112^63 mod 211 = 156

112^64 mod 211 = 170

112^65 mod 211 = 50

112^66 mod 211 = 114

112^67 mod 211 = 108

112^68 mod 211 = 69

112^69 mod 211 = 132

112^70 mod 211 = 14

112^71 mod 211 = 91

112^72 mod 211 = 64

112^73 mod 211 = 205

112^74 mod 211 = 172

112^75 mod 211 = 63

112^76 mod 211 = 93

112^77 mod 211 = 77

112^78 mod 211 = 184

112^79 mod 211 = 141

112^80 mod 211 = 178

112^81 mod 211 = 102

112^82 mod 211 = 30

112^83 mod 211 = 195

112^84 mod 211 = 107

112^85 mod 211 = 168

112^86 mod 211 = 37

112^87 mod 211 = 135

112^88 mod 211 = 139

112^89 mod 211 = 165

112^90 mod 211 = 123

112^91 mod 211 = 61

112^92 mod 211 = 80

112^93 mod 211 = 98

112^94 mod 211 = 4

112^95 mod 211 = 26

112^96 mod 211 = 169

112^97 mod 211 = 149

112^98 mod 211 = 19

112^99 mod 211 = 18

112^100 mod 211 = 117

112^101 mod 211 = 22

112^102 mod 211 = 143

112^103 mod 211 = 191

112^104 mod 211 = 81

112^105 mod 211 = 210

112^106 mod 211 = 99

112^107 mod 211 = 116

112^108 mod 211 = 121

112^109 mod 211 = 48

112^110 mod 211 = 101

112^111 mod 211 = 129

112^112 mod 211 = 100

112^113 mod 211 = 17

112^114 mod 211 = 5

112^115 mod 211 = 138

112^116 mod 211 = 53

112^117 mod 211 = 28

112^118 mod 211 = 182

112^119 mod 211 = 128

112^120 mod 211 = 199

112^121 mod 211 = 133

112^122 mod 211 = 126

112^123 mod 211 = 186

112^124 mod 211 = 154

112^125 mod 211 = 157

112^126 mod 211 = 71

112^127 mod 211 = 145

112^128 mod 211 = 204

112^129 mod 211 = 60

112^130 mod 211 = 179

112^131 mod 211 = 3

112^132 mod 211 = 125

112^133 mod 211 = 74

112^134 mod 211 = 59

112^135 mod 211 = 67

112^136 mod 211 = 119

112^137 mod 211 = 35

112^138 mod 211 = 122

112^139 mod 211 = 160

112^140 mod 211 = 196

112^141 mod 211 = 8

112^142 mod 211 = 52

112^143 mod 211 = 127

112^144 mod 211 = 87

112^145 mod 211 = 38

112^146 mod 211 = 36

112^147 mod 211 = 23

112^148 mod 211 = 44

112^149 mod 211 = 75

112^150 mod 211 = 171

112^151 mod 211 = 162

112^152 mod 211 = 209

112^153 mod 211 = 198

112^154 mod 211 = 21

112^155 mod 211 = 31

112^156 mod 211 = 96

112^157 mod 211 = 202

112^158 mod 211 = 47

112^159 mod 211 = 200

112^160 mod 211 = 34

112^161 mod 211 = 10

112^162 mod 211 = 65

112^163 mod 211 = 106

112^164 mod 211 = 56

112^165 mod 211 = 153

112^166 mod 211 = 45

112^167 mod 211 = 187

112^168 mod 211 = 55

112^169 mod 211 = 41

112^170 mod 211 = 161

112^171 mod 211 = 97

112^172 mod 211 = 103

112^173 mod 211 = 142

112^174 mod 211 = 79

112^175 mod 211 = 197

112^176 mod 211 = 120

112^177 mod 211 = 147

112^178 mod 211 = 6

112^179 mod 211 = 39

112^180 mod 211 = 148

112^181 mod 211 = 118

112^182 mod 211 = 134

112^183 mod 211 = 27

112^184 mod 211 = 70

112^185 mod 211 = 33

112^186 mod 211 = 109

112^187 mod 211 = 181

112^188 mod 211 = 16

112^189 mod 211 = 104

112^190 mod 211 = 43

112^191 mod 211 = 174

112^192 mod 211 = 76

112^193 mod 211 = 72

112^194 mod 211 = 46

112^195 mod 211 = 88

112^196 mod 211 = 150

112^197 mod 211 = 131

112^198 mod 211 = 113

112^199 mod 211 = 207

112^200 mod 211 = 185

112^201 mod 211 = 42

112^202 mod 211 = 62

112^203 mod 211 = 192

112^204 mod 211 = 193

112^205 mod 211 = 94

112^206 mod 211 = 189

112^207 mod 211 = 68

112^208 mod 211 = 20

112^209 mod 211 = 130

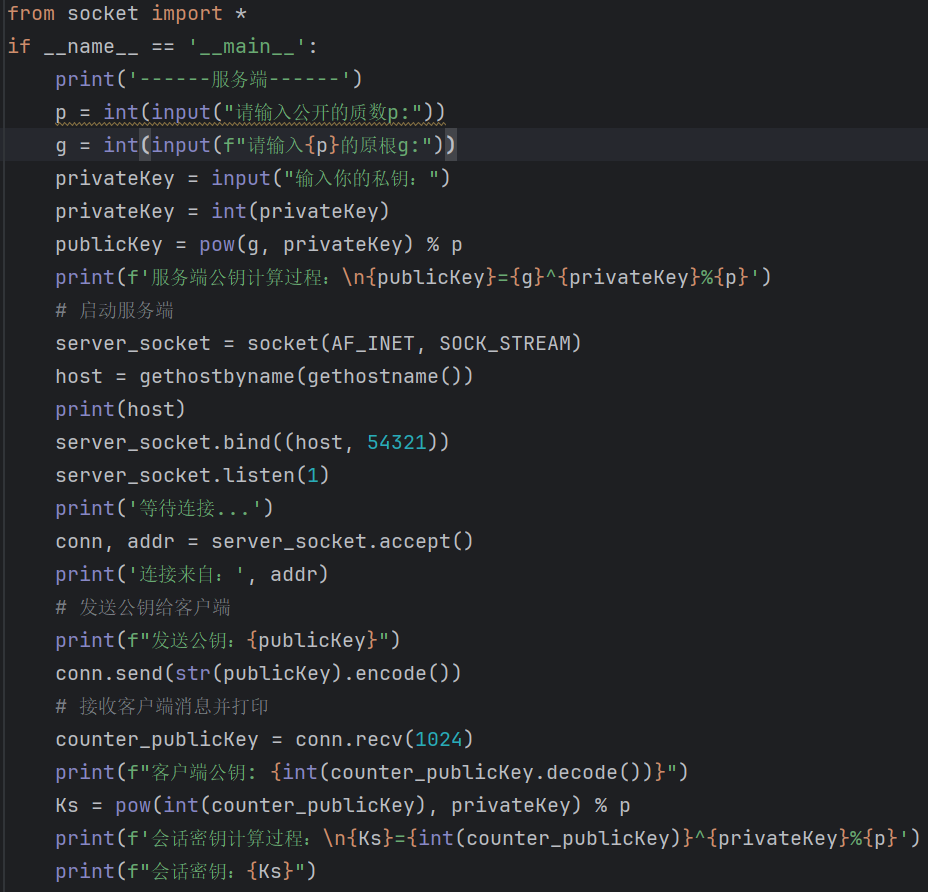
112^210 mod 211 = 1

最终判断：112是211的一个原根

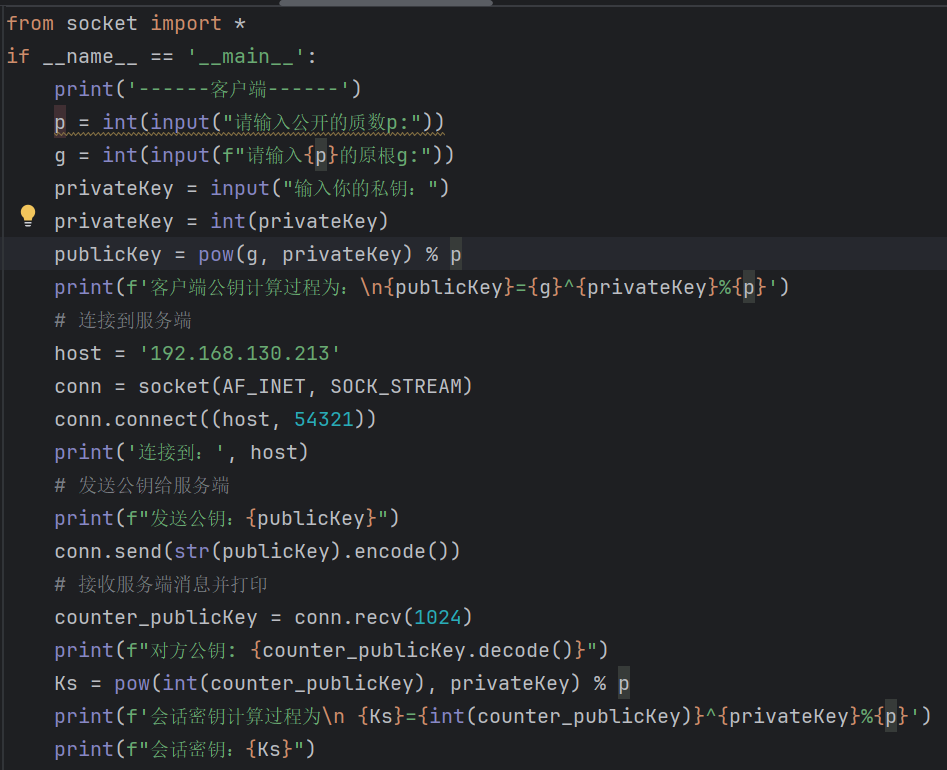
1. **H协议机制流程**

选取质数211和原根112（即p=211 g=112）

服务端

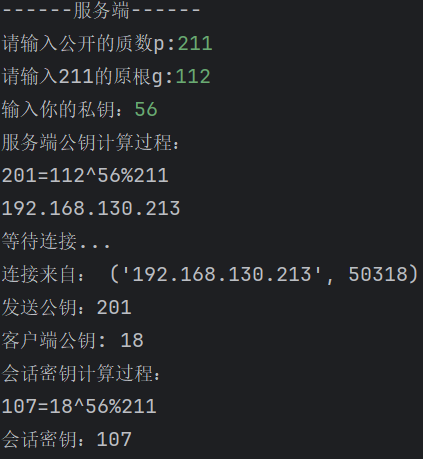


客户端



运行结果：

服务端



客户端

