Problem # 1

Compute the following Legendre's symbols:

a) $\left(\frac{128}{5}\right)$, b) $\left(\frac{35}{7}\right)$, c) $\left(\frac{56}{13}\right)$

a) $\left(\frac{128}{5}\right)=\left(\frac{128(mod\,5)}{5}\right)=\left(\frac{3}{5}\right)$ 5 and 3 are different primes →

$(\frac{3}{5})=(\frac{5}{3})\cdot(-1)^{\frac{3-1}{2}\cdot\frac{5-1}{2}}=1$

b) $\left(\frac{35}{7}\right)=(\frac{35(mod\,7)}{7})=(\frac{0}{7})$

c) $\left(\frac{56}{13}\right)=\left(\frac{56(mod\,13)}{13}\right)=(\frac{4}{13})=(\frac{2}{13})\cdot(\frac{2}{13})=1$

p \ a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
3	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0
5	1	−1	−1	1	0	1	−1	−1	1	0	1	−1	−1	1	0	1	−1	−1	1	0	1	−1	−1	1	0	1	−1	−1	1	0
7	1	1	−1	1	−1	−1	0	1	1	−1	1	−1	−1	0	1	1	−1	1	−1	−1	0	1	1	−1	1	−1	−1	0	1	1
11	1	−1	1	1	1	−1	−1	−1	1	−1	0	1	−1	1	1	1	−1	−1	−1	1	−1	0	1	−1	1	1	1	−1	−1	−1
13	1	−1	1	1	−1	−1	−1	−1	1	1	−1	1	0	1	−1	1	1	−1	−1	−1	−1	1	1	−1	1	0	1	−1	1	1
17	1	1	−1	1	−1	−1	−1	1	1	−1	−1	−1	1	−1	1	1	0	1	1	−1	1	−1	−1	−1	1	1	−1	−1	−1	1
19	1	−1	−1	1	1	1	1	−1	1	−1	1	−1	−1	−1	−1	1	1	−1	0	1	−1	−1	1	1	1	1	−1	1	−1	1
23	1	1	1	1	−1	1	−1	1	1	−1	−1	1	1	−1	−1	1	−1	1	−1	−1	−1	−1	0	1	1	1	1	−1	1	−1
29	1	−1	−1	1	1	1	1	−1	1	−1	−1	−1	1	−1	−1	1	−1	−1	−1	1	−1	1	1	1	1	−1	−1	1	0	1
31	1	1	−1	1	1	−1	1	1	1	1	−1	−1	−1	1	−1	1	−1	1	1	1	−1	−1	−1	−1	1	−1	−1	1	−1	−1
37	1	−1	1	1	−1	−1	1	−1	1	1	1	1	−1	−1	−1	1	−1	−1	−1	−1	1	−1	−1	−1	1	1	1	1	−1	1
41	1	1	−1	1	1	−1	−1	1	1	1	−1	−1	−1	−1	−1	1	−1	1	−1	1	1	−1	1	−1	1	−1	−1	−1	−1	−1
43	1	−1	−1	1	−1	1	−1	−1	1	1	1	−1	1	1	1	1	1	−1	−1	−1	1	−1	1	1	1	−1	−1	−1	−1	−1
47	1	1	1	1	−1	1	1	1	1	−1	−1	1	−1	1	−1	1	1	1	−1	−1	1	−1	−1	1	1	−1	1	1	−1	−1
53	1	−1	−1	1	−1	1	1	−1	1	1	1	−1	1	−1	1	1	1	−1	−1	−1	−1	−1	−1	1	1	−1	−1	1	1	−1
59	1	−1	1	1	1	−1	1	−1	1	−1	−1	1	−1	−1	1	1	1	−1	1	1	1	1	−1	−1	1	1	1	1	1	−1
61	1	−1	1	1	1	−1	−1	−1	1	−1	−1	1	1	1	1	1	−1	−1	1	1	−1	1	−1	−1	1	−1	1	−1	−1	−1
67	1	−1	−1	1	−1	1	−1	−1	1	1	−1	−1	−1	1	1	1	1	−1	1	−1	1	1	1	1	1	1	−1	−1	1	−1
71	1	1	1	1	1	1	−1	1	1	1	−1	1	−1	−1	1	1	−1	1	1	1	−1	−1	−1	1	1	−1	1	−1	1	1
73	1	1	1	1	−1	1	−1	1	1	−1	−1	1	−1	−1	−1	1	−1	1	1	−1	−1	−1	1	1	1	−1	1	−1	−1	−1
79	1	1	−1	1	1	−1	−1	1	1	1	1	−1	1	−1	−1	1	−1	1	1	1	1	1	1	−1	1	1	−1	−1	−1	−1
83	1	−1	1	1	−1	−1	1	−1	1	1	1	1	−1	−1	−1	1	1	−1	−1	−1	1	−1	1	−1	1	1	1	1	1	1
89	1	1	−1	1	1	−1	−1	1	1	1	1	−1	−1	−1	−1	1	1	1	−1	1	1	1	−1	−1	1	−1	−1	−1	−1	−1
97	1	1	1	1	−1	1	−1	1	1	−1	1	1	−1	−1	−1	1	−1	1	−1	−1	−1	1	−1	1	1	−1	1	−1	−1	−1
101	1	−1	−1	1	1	1	−1	−1	1	−1	−1	−1	1	1	−1	1	1	−1	1	1	1	1	1	1	1	−1	−1	−1	−1	1
103	1	1	−1	1	−1	−1	1	1	1	−1	−1	−1	1	1	1	1	1	1	1	−1	−1	−1	1	−1	1	1	−1	1	1	1
107	1	−1	1	1	−1	−1	−1	−1	1	1	1	1	1	1	−1	1	−1	−1	1	−1	−1	−1	1	−1	1	−1	1	−1	1	1
109	1	−1	1	1	1	−1	1	−1	1	−1	−1	1	−1	−1	1	1	−1	−1	−1	1	1	1	−1	−1	1	1	1	1	1	−1
113	1	1	−1	1	−1	−1	1	1	1	−1	1	−1	1	1	1	1	−1	1	−1	−1	−1	1	−1	−1	1	1	−1	1	−1	1
127	1	1	−1	1	−1	−1	−1	1	1	−1	1	−1	1	−1	1	1	1	1	1	−1	1	1	−1	−1	1	1	−1	−1	−1	1

Problem # 2

Compute the following Jacobi's symbols:

a) $\left(\frac{56}{15}\right)$, b) $\left(\frac{13}{25}\right)$, c) $\left(\frac{57}{21}\right)$, d) $\left(\frac{13}{35}\right)$, e) $\left(\frac{12}{45}\right)$

a) $\left(\frac{56}{15}\right)=\left(\frac{56(mod\,15)}{15}\right)=(\frac{11}{15})=(\frac{11}{5})\cdot(\frac{11}{3})=1\cdot(-1)=-1$

b) $\left(\frac{13}{25}\right)=\left(\frac{13}{5}\right)^2=1^2=1$

c) $\left(\frac{57}{21}\right)=(\frac{57\,mod\,21}{21})=(\frac{15}{21})=(\frac{15}{3})\cdot(\frac{15}{7})=0$

d) $\left(\frac{13}{35}\right)=(\frac{13}{5})\cdot(\frac{13}{7})=1\cdot1=1$

e) $\left(\frac{12}{45}\right)=(\frac{13}{3})^2\cdot(\frac{12}{5})=0$

n \ k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0
5	1	−1	−1	1	0	1	−1	−1	1	0	1	−1	−1	1	0	1	−1	−1	1	0	1	−1	−1	1	0	1	−1	−1	1	0
7	1	1	−1	1	−1	−1	0	1	1	−1	1	−1	−1	0	1	1	−1	1	−1	−1	0	1	1	−1	1	−1	−1	0	1	1
9	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
11	1	−1	1	1	1	−1	−1	−1	1	−1	0	1	−1	1	1	1	−1	−1	−1	1	−1	0	1	−1	1	1	1	−1	−1	−1
13	1	−1	1	1	−1	−1	−1	−1	1	1	−1	1	0	1	−1	1	1	−1	−1	−1	−1	1	1	−1	1	0	1	−1	1	1
15	1	1	0	1	0	0	−1	1	0	0	−1	0	−1	−1	0	1	1	0	1	0	0	−1	1	0	0	−1	0	−1	−1	0
17	1	1	−1	1	−1	−1	−1	1	1	−1	−1	−1	1	−1	1	1	0	1	1	−1	1	−1	−1	−1	1	1	−1	−1	−1	1
19	1	−1	−1	1	1	1	1	−1	1	−1	1	−1	−1	−1	−1	1	1	−1	0	1	−1	−1	1	1	1	1	−1	1	−1	1
21	1	−1	0	1	1	0	0	−1	0	−1	−1	0	−1	0	0	1	1	0	−1	1	0	1	−1	0	1	1	0	0	−1	0
23	1	1	1	1	−1	1	−1	1	1	−1	−1	1	1	−1	−1	1	−1	1	−1	−1	−1	−1	0	1	1	1	1	−1	1	−1
25	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0
27	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0
29	1	−1	−1	1	1	1	1	−1	1	−1	−1	−1	1	−1	−1	1	−1	−1	−1	1	−1	1	1	1	1	−1	−1	1	0	1
31	1	1	−1	1	1	−1	1	1	1	1	−1	−1	−1	1	−1	1	−1	1	1	1	−1	−1	−1	−1	1	−1	−1	1	−1	−1
33	1	1	0	1	−1	0	−1	1	0	−1	0	0	−1	−1	0	1	1	0	−1	−1	0	0	−1	0	1	−1	0	−1	1	0
35	1	−1	1	1	0	−1	0	−1	1	0	1	1	1	0	0	1	1	−1	−1	0	0	−1	−1	−1	0	−1	1	0	1	0
37	1	−1	1	1	−1	−1	1	−1	1	1	1	1	−1	−1	−1	1	−1	−1	−1	−1	1	−1	−1	−1	1	1	1	1	−1	1
39	1	1	0	1	1	0	−1	1	0	1	1	0	0	−1	0	1	−1	0	−1	1	0	1	−1	0	1	0	0	−1	−1	0
41	1	1	−1	1	1	−1	−1	1	1	1	−1	−1	−1	−1	−1	1	−1	1	−1	1	1	−1	1	−1	1	−1	−1	−1	−1	−1
43	1	−1	−1	1	−1	1	−1	−1	1	1	1	−1	1	1	1	1	1	−1	−1	−1	1	−1	1	1	1	−1	−1	−1	−1	−1
45	1	−1	0	1	0	0	−1	−1	0	0	1	0	−1	1	0	1	−1	0	1	0	0	−1	−1	0	0	1	0	−1	1	0
47	1	1	1	1	−1	1	1	1	1	−1	−1	1	−1	1	−1	1	1	1	−1	−1	1	−1	−1	1	1	−1	1	1	−1	−1
49	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1
51	1	−1	0	1	1	0	−1	−1	0	−1	1	0	1	1	0	1	0	0	1	1	0	−1	1	0	1	−1	0	−1	1	0
53	1	−1	−1	1	−1	1	1	−1	1	1	1	−1	1	−1	1	1	1	−1	−1	−1	−1	−1	−1	1	1	−1	−1	1	1	−1
55	1	1	−1	1	0	−1	1	1	1	0	0	−1	1	1	0	1	1	1	−1	0	−1	0	−1	−1	0	1	−1	1	−1	0
57	1	1	0	1	−1	0	1	1	0	−1	−1	0	−1	1	0	1	−1	0	0	−1	0	−1	−1	0	1	−1	0	1	1	0

59 1 −1 1 1 1 −1 1 −1 1 −1 −1 1 −1 −1 1 1 1 −1 1 1 1 1 −1 −1 1 1 1 1 1 −1

Problem #3 Verify if the following congruencies have solutions

a) $x^2 \equiv 127(mod\,13) \rightarrow (\frac{10}{3}) = 1 \rightarrow$ Has solutions → X=6

Let's consider y=x^2 For an easier calculation we have the following Fact for each positive integer n: a and b integers

First, consider d=gcd (a,m). The congruence equation $ax \equiv b(mod\, n)$ has a solution x if and only it d divides b, in which case there are exactly d solutions between o and n-1; these solution are all congruent modulo $\frac{n}{d}$

127 (mod 13)=10 we for x^2 (mod 13)=127

Considering x=a, we can check for every number between 0 and 12

$a \equiv b(mod\, n)$ → n divides (a-b) a is congruent to be fulfilling this 13 divides x^2 -127, we con verify every number be (cw 12 for

The only combination witn $x^2 > 127$ is 12·12=144 144-127=17, which can 4 be divided by 13 so no solution

b) $x^2 \equiv 8(mod\,17) \rightarrow (\frac{8}{17}) = 1 \rightarrow$ Has solutions → X=5

x^2 =ax → x^2-8 should be divided by 17, and $x^2 \in (0,16)$

x^2 =5·5=25 → 17, which can be divided by 17

gcd=(5,17)=1 Just one solution and we already found it

Also x^2 =12·12 is a solution 12·12-8=136=8(mod 17)

$25 \equiv 8(mod\,17)$ $148 \equiv 8(mod\,17)$

http://www.numbertheory.org/php/squareroot.php
http://www.a-calculator.com/congruence/

Problem #4 Give an example of a pseudoprime number

First we are going to define a pseudoprime number:
Let n be an odd composite integer and (et “a” be an integer, $1 \leq a \leq n-1$
Then n is said to be a pseudoprime to the base a it $a^{n-1} \equiv (mod\, n)$.

a) to the base 3
n-1>=a → n= a+1 → n>4
$a1 = 7 \cdot 13 \rightarrow 3^{90}(mod\, 91)$ → $3^{90} \equiv 1(mod\, 91)$

b) to the base 5
$5^{123} \equiv 1(mod\, 124)$ $124 = 2^2 .31$

Euler pseudoprime to the base a
If gcd (a.n)=1 and $a^{(n-1)/2} \equiv (\frac{a}{n})(mod\, n)$, n is a pseudoprime to the base a
To the base 3 → 121=n
To the base 5 → 217
If either $a^r \equiv 1$

Problem # 5
Assume $k \in N$ and $GF(2^k)[x]$ is a ring of polynomials with coefficients in the field $GF(2^k)$. Prove, that if $r \in N$, $n \in N$, $n \geq 2$ and x^r is a polynomial from the ring of polynomials $GF(2^k)[x]$, then we have $x^r(mod(x^n+1)) = x^{r(mod\, n)}$

In $Z_2 = \{0,1\}$ $1 \oplus 1 = 0$ and $0 \oplus 0 = 0$, so – a=a for $a \in Z_2$ and $a -_2 b = a \oplus b$ where $-_2$ is a modulo 2 subtraction.
$a = a_1, a_2, \ldots a_k \in GF(2^k)$ where $a_i \in \{0,1\}$ and $b = b_1, b_2, \ldots b_k \in GF(2^k)$ where $b_i \in \{0,1\}$ $a+b = \{a_1 \oplus_2 b_1, a_2 \oplus_2 b_2, \ldots a_k \oplus_2 b_k\}$ and the same is for $a -_2 b$
For r<4 equation is always true and for $n \geq 2$ there exists such $q \in N$ that $m = q \cdot r + n$ where $m \equiv r(mod\, n)$
Also we observe dividing polynomial x^n for $n \geq 4$, stating that Z_2 addition and subtraction are identical

$x^{r-4}+x^{r-8}+\dots+x^{n-4\cdot n} \div x^{4}+1$ ~~Very~~ Proved (?)

x^{r}

$x^{r}+x^{r-4}$

x^{r-4}

$x^{r-4}+x^{r-8}$

$\dots$

x^{r}

Problem # 6

Propose a Shamir's algorithm of secret sharing for n = 5 users and the threshold t = 3 . Compute shares of all users for a secret 8.

<u>1) Setup</u>. The trusted party T begins with a secret integers=8 it wishes to distribute among n= 5 users

a) T chooses a prime p>max (8,5), for example p=11, and defines $u_0=5$

b) T selects t-1=2 random, independent coefficients

$a_1,\dots,a_{t-1}, 0\le a; \le p-1$

$a_1=4, a_2=10$

and defines the random polynomial over Z_p

$F(x)=4x+10x^2+5$ Bad!!! (y firgit ao)

c) T computes S_i= F(i) mod p, $1\le i\le n$ (or for any n vistonct points, $1\le c\le p-1;$

$S_1=14\, mod\, 11=3;$

$S_2=48\, mod\, 11=4$

$S_3=102\, mod\, 11=3$

$S_4=176\, mod\, 11=0$

$S_5=270\, mod\, 11=6$

Securely transfers the share S_0 to user P_i , along with public index i.

2)<u>Pooling of shares</u>

Any group of t=3 or more users pool their shares provide 3 distinct points $(x,y)=(i,s_i)$ allowing computation of the coefficients $a_j \quad 1 \le t \le t-1$ of f(x) by Lagrange interpolation- the secret is recovered → f(0)=a^0=S F(0)= 5=5

Problem # 7

Propose a Shamir's algorithm of secret sharing for n = 6 users and the threshold t = 4 . Compute shares of all users for a secret 10.

a) T chooses a prime p>max(10,6) → p=11, and defines

$a_0=6, a_1=2, a_2=3, a_3=5$

b) Selection of 3 random independent coefficients: And definition of the random polynomial over Z_p

$F(x)=6+2x+3x^2+5x^3$

c) T computes and securety transfers the following shares S_i to users $P_i \quad 1 \le i \le 6$

$S_1=(6+2+3+5)(mod\,11)=16\,Mod\,11=5$

$S_2=6+2\cdot 2+3\cdot 2^2+5.2^3=62\,mod\,11=7$

$S_3=174\,mod\,11=9$

$S_4=382\,mod\,11=8$

$S_5=716\,mod\,11=1$

$S_6=1206\,mod\,11=7$

Problem # 7

Design a public key cryptosystem RSA for "small numbers". Cipher an exemplary plain text message and decipher obtained cryptogramme.

We are going to dive directly an example:

Alice chooses the primes p=2357, q=2551, and computes n=pq=6012707 and $\phi=(p-1)(q-1)=6007800$ Alice chooses e=3674911 and, using the extended Euclidean Algorithm, Finds d=422141 such that $ed \equiv 1(mod\,\phi)$. Alice's Public key is the pair (n=6012707, e=3674911), while Alice's private key is d=422191

Encryption

Too encrypt is message m=5234673, Bob uses an algorithm for modular exponentiation to compute

$c=m^e\,mod\,n=5234673^{3674411}\,mod\,6012707=3656502$; and gends this to A.

Decryption

To decrypt c, A computes

$c^d \, mod \, n = 3650502^{422141} \, mod \, 3012707 = 5234673$

Problem # 8
Design a public key cryptosystem ElGamal for “small numbers”. Cipher an exemplary plain text message and decipher obtained cryptogramme.

<u>Key generation</u>
Alice selects the prime p=2357 and a generator $\alpha=2$ of Z^*_{2357} .
Alice chooses the private key n=1751 and computes
$\alpha^a \, mod \, p = 2^{1751} \, mod \, 2357 = 1185$
Alice's public key is $(p=2357, \alpha=2, \alpha^a=1185)$
<u>Encryption</u>
To encrypt a message m=2035, Bob selects a random integer k=1520 and computes
$\alpha = 2^{1520} \, mod \, 2357 = 1430$
$g = 2035 \cdot 1185^{1520} \, mod \, 2357 = 697$
Bob sends $\alpha=1430$ and g=647 to Alice
<u>Description</u>
To decrypt, Alice computes
$\alpha^{p-1-a} = 1430^{605} \, mod \, 2357 = 872$
and recovers m by computing m=872·647 mod 2357=2035

Problem # 9
Design an ElGamal signature algorithm for “small numbers”. Sign an exemplary plain text message and verify correctness of the signature.

<u>Key generation</u>
Alice selects the prime p=2357 and a generator $\alpha=2$ of Z^*_{2357} .
Alice chooses the private key a=1751 and computes
$y = \alpha^a \, mode \, p = 2^{1751} \, mod \, 2357 = 1185$. Alice’s public key is (p=2357, x=z, y=1185)
<u>Signature generation</u>
For simplicity, messages will be integers from Z^p and h(m)=m (i.e For this example only, take n to be the identity function) To sign the message m=1436,Alice selects a random integer k=1529, computes $r = \alpha^k \, mod \, p = 2^{1524} \, mod \, 2357 = 1440$, and $k^{-1} \, mod (p^{-1}) = 245$. Finally, Alice computes $S = 245(1463 - 1751(1490)) \, mod \, 2356 = 1777$ Alice’s signature for n=1463 is the pair (r=1490, s=1777)

Signature verification

Bob computes $v_1 = 1185^{1490} \cdot 1490^{1777} \, mod \, 2357 = 1072$, h(m)=1463, $v_2 = 2^{1463} \, mod \, 2357 = 1072$. Bob accepts the signature since $v_1 = v_2$