The new cryptological system and other results related to the discovery of number theory

Ivo Považan
pensioner
Slovakia
Bratislava
e-mail: i.povazan@upcmail.sk
mobil: +421-944-662-674

Version 0.9

28. mája 2017

Function $\chi(n)$

We define the following functions $\chi(n)$:

$$\text{For a prime } p = 4k+1, \chi(p) = p-1,$$

$$\text{For a prime } q = 4k-1, \chi(q) = q+1,$$

$$\chi(p^\alpha) = p^{\alpha-1}(p-1)$$

$$\chi(q^\alpha) = q^{\alpha-1}(q+1)$$

$$\chi(2^\alpha) = 2^{\alpha-1}$$

$$\text{If } \gcd(m,n) = 1, \text{ then } \chi(mn) = \chi(m)\chi(n).$$

Function $\chi(n)$ is similar to Euler's totient function.

Binary Quadratic Forms

Binary Quadratic Forms:

$$\mathbf{q} = ax^2 + bxy + cy^2$$

Discriminants of Forms:

$$\Delta = b^2 - 4ac.$$

Next we will only work with forms:

$$\Delta = -(2dN)^2 \quad N \text{ is odd a } d = 2^0, 2^1, 2^2, \ldots$$

Principal Forms:

$$(1, 0, -\frac{\Delta}{4}) \text{ - we will label it } \mathbf{1}.$$

A form (a, b, c) is said to be primitive if:

$$\gcd(a, b, c) = 1$$

A form (a, b, c) is said to be ambiguous if:

$$(a, b, c) \text{ is equivalent to } (a, -b, c)$$

The class number $h(\Delta)$ is the number of proper equivalence classes of primitive integral forms of discriminant Δ.
Classnumber:

$$\mathbf{cl} = \chi\left(\frac{dN}{2}\right) \tag{1}$$

and

$$\mathbf{q}^{\mathbf{cl}} = \mathbf{1} \tag{2}$$

A special case:
If N is a prime of type $p = 4k + 1$ and $d = 2$,

$$\mathbf{q}^{p-1} = \mathbf{1} \tag{3}$$

If N is a prime of type $p = 4k - 1$ and $d = 2$,

$$\mathbf{q}^{p+1} = \mathbf{1} \tag{4}$$

The sketch of the proof is in the examples 1 and 2, which are in the next section.

Composition of Forms

$$m = \gcd\left(a_2, a_1, \frac{b_1 + b_2}{2}\right)$$

and

$$a = \frac{a_1 a_2}{m^2}$$

Moreover, *let* $j, k, l \in Z$ such that

$$m = ja_2 + ka_1 + l\frac{b_2 + b_1}{2}$$

$$b \equiv \frac{ja_2 b_1 + ka_1 b_2 + l\frac{b_1 b_2 + \Delta}{2}}{m} \mod 2a$$

$$c = \frac{b^2 - \Delta}{4a}$$

.

Canonic Form

$$\Delta = b^2 - 4ac$$

$$\Delta = -(2 \cdot d \cdot N)^2$$

$$4ac = b^2 - \Delta$$

if $b = 2kN$ than

$$4ac = 4k^2N^2 + 4 \cdot d^2 \cdot N^2$$

$$a = N^2$$

$$c = k^2 + d^2$$

In most cases, the composition of two forms can be reduced to the calculation of k_3.

$$Qfb(N^2, 2k_1 N, d^2 + k_1^2) \cdot Qfb(N^2, 2k_2 N, d^2 + k_2^2) = Qfb(N^2, 2k_3 N, d^2 + k_3^2)$$

$$k_3 = \frac{k_1 k_2 - d^2}{k_1 + k_2} \mod N \tag{5}$$

The following equations are given for interest.

$$K_3 = (k_1 + d\,\mathbf{i})\,(k_2 + d\,\mathbf{i})$$

$$\Re(K_3) = k_1\,k_2 - d^2$$

$$\Im(K_3) = d\,k_2 + d\,k_1$$

Exampe 1: $d = 2, N = 127, N\%4 = 3$ N is prime.

k	$Qfb(N^2, 2kN, d^2 + k^2)$	reduced form
1	Qfb(16129, 254, 5)	Qfb(5, -4, 12904)
2	Qfb(16129, 508, 8)	Qfb(8, 4, 8065)
3	Qfb(16129, 762, 13)	Qfb(13, -8, 4964)
4	Qfb(16129, 1016, 20)	Qfb(20, -16, 3229)
⋮		
124	Qfb(16129, 31496, 15380)	Qfb(13, 8, 4964)
125	Qfb(16129, 31750, 15629)	Qfb(8, -4, 8065)
126	Qfb(16129, 32004, 15880)	Qfb(5, 4, 12904)
127	Qfb(16129, 32258, 16133)	Qfb(4, 0, 16129)
128	Qfb(16129, 32512, 16388)	Qfb(5, -4, 12904)
129	Qfb(16129, 32766, 16645)	Qfb(8, 4, 8065)
130	Qfb(16129, 33020, 16904)	Qfb(13, -8, 4964)
131	Qfb(16129, 33274, 17165)	Qfb(20, -16, 3229)

Exampe 2: $d = 2, N = 101, N\%4 = 1$ N is prime.

k	$Qfb(N^2, 2kN, d^2 + k^2)$	reduced form
1	Qfb(10201, 202, 5)	Qfb(5, -2, 8161)
2	Qfb(10201, 404, 8)	Qfb(8, -4, 5101)
3	Qfb(10201, 606, 13)	Qfb(13, -8, 3140)
⋮		
20	Qfb(10201, 4040, 404)	Qfb(101, 0, 404)
21	Qfb(10201, 4242, 445)	Qfb(116, 24, 353)
⋮		
80	Qfb(10201, 16160, 6404)	Qfb(116, -24, 353)
81	Qfb(10201, 16362, 6565)	Qfb(101, 0, 404)
⋮		
100	Qfb(10201, 20200, 10004)	Qfb(5, 2, 8161)
101	Qfb(10201, 20402, 10205)	Qfb(4, 0, 10201)
102	Qfb(10201, 20604, 10408)	Qfb(5, -2, 8161)

Reduced binary quadratic form is repeated with period N.
The principal form is not there and therefore needs to be added.
We have $N+1$ forms. It only applies if $N \equiv 3 \mod 4$.

If $N \equiv 1 \mod 4$ then in each period there are two forms that are not primitive. We have $N-1$ forms.
N can be expressed as $N = a^2 + b^2$.

Cryptologic system

$$N = pq$$

$$ed \equiv 1 \mod \chi(N)$$

$$ed = 1 + k\chi(N)$$

$$\mathbf{q}^{ed} = \mathbf{q}^1 \mathbf{q}^{(k\chi(N))}$$

$$(\mathbf{q}^e)^d = \mathbf{q}$$

Conjecture:

Let $N = 4k - 1$ *be a natural number . N is prime if and only if:*

$$2^{N-1} \equiv 1 \mod N \tag{6}$$

and

$$\mathbf{q}^{N+1} = \mathbf{1} \tag{7}$$

Programs for Test

All test programs are written in PARI / GP language.
Usage is in source code comments.
1.file **phb.gp** - public-key cryptosystems.
2.file **pr.gp** - primality test.
3.file **poll.gp** - integer factorization.
4.file **mer.gp** - primality test for Mersenne numbers.
5.file **fchi.gp** - Compare $\chi()$ and classnumber() functions.