NEW ABELIAN GROUPS FOR PRIMES OF TYPE $4K-1$ AND $4K+1$.

Anna Považanová
Faculty of Informatics and Information Technologies,
SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA, Slovakia
anna.povazanova@stuba.sk

Ivo Považan
to May 2012 Institute of Informatics, SLOVAK ACADEMY OF SCIENCES,
Bratislava, Slovakia
i.povazan@upcmail.sk

Abstract

p is prime.The article describes the new Abelian groups of type $p = 4k+1$ and $p = 4k-1$, for which a theorem similar to the Fermat's little theorem applies. The multiplicative group $(Z/pZ)^*$ in some sense similar to the Abelian group of type $p = 4k+1$. Abelian group of type $p = 4k-1$ is a different structure compared to group $(Z/pZ)^*$. This fact is used for the primality test of integer $N = 4k-1$. The primality test was verified up to $N = 2^{64}$.

1 Introduction

The main goal of the article is to present new Abelian groups. One of the applications of these groups is a primality test. The main inspiration comes from [8].
In the article we use the language of elementary terms. Proofs are informal, but we believe it can be translated into a formal language. The main part of the article is based on an operation which is a group operation and the elements of the group are the extended equivalent classes - unordered pairs.
When defining a group, we only work with primes of the $p = 4k-1$ or $p = 4k+1$ type.
For each type of prime, Abelian groups have a different formula for the number of elements.

For both types of groups,there is valid the analogous theorems of the Fermat's little theorem.

2 Equivalence Classes and Groups

An equivalence class [7] is defined as a subset of the form $\{x \in X : xRa\}$, where a is an element of X and the notation "xRy" is used to mean that there is an equivalence relation between x and y. It can be shown that any two equivalence classes are either equal or disjoint, hence the collection of equivalence classes forms a partition of X. For all $a, b \in X$, we have aRb if and only if a and b belong to the same equivalence class.
A set of class representatives is a subset of X which contains exactly one element from each equivalence class.

For prime p and a, b integers, consider the congruence

$$a \equiv b \pmod{p} \qquad aRb \tag{1}$$

then the equivalence classes are the sets $\{..., -2p, -p, 0, p, 2p, ...\}$, $\{..., 1-2p, 1-p, 1, 1+p, 1+2p, ...\}$ etc. The standard class representatives are taken to be $\{\{0\}, \{1\}, \{2\}, ..., \{p-1\}\}$.

$a \neq 0$, $b \neq 0$ and a, b are class representatives. If

$$ab \equiv -1 \pmod{p} \qquad aSb \tag{2}$$

then

$$(a + k_1 p)(b + k_2 p) \equiv -1 \pmod{p}$$

Relations R (1) is reflexive, symmetric, and transitive. They are generally called equivalence relations. Relation S (2) for prime $p = 4k - 1$ is only symmetric except for 0. Relation S (2) for prime $p = 4k + 1$ is only symmetric except for 0 and two other members.

Definition 1. *According to [6]*

$$T = R \cup S \tag{3}$$

Definition 2.

$$0 \cdot \infty \equiv -1 \pmod{p} \tag{4}$$

Definition 3. *$n \in \mathbb{N}$ and $n \neq 0$*

$$0 = \frac{n}{\infty} \text{ and } \infty = \frac{n}{0} \tag{5}$$

Lemma 1. *p is prime. $x^2 \equiv -1 \pmod p$ if and only if $p \equiv 1 \pmod 4$*

Relation T is equivalence.
When $p = 4k - 1$ then the T relation generates $\frac{p+1}{2}$ class representatives,who have 2 members.
When $p = 4k + 1$ then the T relation generates $\frac{p-1}{2}$ class representatives,who have 2 members.

Example 1. *Prime $p = 4k + 1$.For $p = 17$, the class representatives of the T relation are as follows.*

$\{0, \infty\}, \{1, 16\}, \{2, 8\}, \{3, 11\}, \{4\}, \{5, 10\}, \{6, 14\}, \{7, 12\}, \{9, 15\}, \{13\}$

If is $x = 4$ or $x = 13$ then is valid $x^2 \equiv -1(\bmod p)$.

Example 2. *Prime $p = 4k - 1$.For $p = 19$, the class representatives of the T relation are as follows.*

$\{0, \infty\}, \{1, 18\}, \{2, 9\}, \{3, 6\}, \{4, 14\}, \{5, 15\}, \{7, 8\}, \{10, 17\}, \{11, 12\}, \{13, 16\}$

We have a prime p and a binary operation

$$x_3 \equiv \frac{x_1 x_2 - 1}{x_1 + x_2} \pmod p \tag{6}$$

This operation (6) is a group operation. The elements of the group are the extended equivalence classes that generate T, they are unordered pair. This operation (6) is commutative because the addition and multiplication is commutative.
Closure:
1.
$$\frac{x_1 x_2 - 1}{x_1 + x_2} = x_3$$
2.
$$\frac{\frac{-1}{x_1}\frac{-1}{x_2} - 1}{\frac{-1}{x_1} + \frac{-1}{x_2}} = \frac{\frac{1 - x_1 x_2}{x_1 x_2}}{\frac{-x_1 - x_2}{x_1 x_2}} = \frac{x_1 x_2 - 1}{x_1 + x_2} = x_3$$
3.
$$\frac{\frac{-1}{x_1} x_2 - 1}{\frac{-1}{x_1} + x_2} = \frac{\frac{-x_2 - x_1}{x_1}}{\frac{-1 + x_1 x_2}{x_1}} = \frac{-(x_1 + x_2)}{x_1 x_2 - 1} = \frac{-1}{x_3}$$
$x_3, \frac{-1}{x3}$ belong to the same equivalence class.

Associativity:
By direct insertion into binary operation, we can easily prove that the operation is associative
Identity element:$\{0, \infty\}$
1.
0 is the identity element.

$$x_3 \equiv \frac{0 \cdot x_2 - 1}{0 + x_2} \pmod{p} \quad x_2 x_3 \equiv -1 \pmod{p}$$

x_2, x_3 belong to the same equivalence class.
2.
∞ is the identity element.

$$x_2 \equiv \frac{x_1 x_2 - 1}{x_1 + x_2} = \frac{x_2 - \frac{1}{x_1}}{1 + \frac{x_2}{x_1}} = \frac{x_2 - \frac{1}{\infty}}{1 + \frac{x_2}{\infty}} \pmod{p}$$

Inverse element:
If $x_1 x_2 \equiv 1 \pmod{p}$ or $x_1 + x_2 \equiv 0 \pmod{p}$ then x_1, x_2 are inverse elements.
1.
If $x_1 x_2 \equiv 1 \pmod{p}$ then

$$0 \equiv \frac{1 - 1}{x_1 + x_2} \pmod{p}$$

2.
If $x_1 + x_2 \equiv 0 \pmod{p}$ then

$$\infty \equiv \frac{x_1 x_2 - 1}{0} \pmod{p}$$

Explicitness:

$$\gcd(x_1 + x_2, p) \neq p \text{ and } \gcd(x_1 + x_3, p) \neq p$$

$$\frac{x_1 x_2 - 1}{x_1 + x_2} \equiv \frac{x_1 x_3 - 1}{x_1 + x_3} \pmod{p} \tag{7}$$

$$x_1^2 (x_2 - x_3) \equiv -(x_2 - x_3) \pmod{p} \tag{8}$$

For prime $p = 4k - 1$ equation (8) has a solution if equality

$$x_2 - x_3 \equiv 0 \pmod{p}$$

For prime $p = 4k + 1$ equation (8) has a solution if equality

$$x_2 - x_3 \equiv 0 \pmod{p} \quad or \quad x_1^2 \equiv -1 \pmod{p}$$

If $x_1^2 \equiv -1 \pmod{p}$ then x_1 is not elements of the group.

Lemma 2. *If $p = 4k - 1$ then group has $\frac{p+1}{2}$ elements.*

Lemma 3. *If $p = 4k + 1$ then group has $\frac{p-1}{2}$ elements.*

The groups are Abelian groups and they are cyclic.
Every infinite cyclic group is isomorphic to the additive group of $\mathbf{Z}$, the integers.
Every finite cyclic group of order n is isomorphic to the additive group of $\mathbf{Z}/n\mathbf{Z}$, the integers modulo n [17, 18, 19].

$$\text{arcCot}(x_1) + \text{arcCot}(x_2) = \text{arcCot}\left(\frac{x_1 x_2 - 1}{x_1 + x_2}\right) \tag{9}$$

When we know the prime factorization of the numbers $\frac{p+1}{2}$ and $\frac{p-1}{2}$ then we can easily find the generator of the given cyclic groups.

In a group G with operation $*$ $(\frac{x_1 x_2 - 1}{x_1 + x_2})$ we will use:

$$a^x = \overbrace{a * a * \cdots * a * a}^{x \ terms}$$

Theorem 1. *If p is prime $p = 4k - 1$ then*

$$a^{(p+1)/2} = identity\ element \tag{10}$$

Theorem 2. *If p is prime $p = 4k + 1$ then*

$$a^{(p-1)/2} = identity\ element \tag{11}$$

In equations (10),(11), the group operation is $x_3 \equiv \frac{x_1 x_2 - 1}{x_1 + x_2} \pmod{p}$.
Theorems (1), (2) are analogous to the Fermat's little theorem.

Example 3. *Element* $\{1, p-1\}$ *has order* 2.

It is valid: $1 \cdot (p-1) (\bmod p) \equiv -1$

a. $\frac{1 \cdot 1 - 1}{1+1} = 0$ *Identity element.*

b. $\frac{1 \cdot (p-1) - 1}{1 + (p-1)} = \frac{p-2}{0} = \infty$ *Identity element.*

c. $\frac{(p-1) \cdot 1 - 1}{(p-1)+1} = \frac{p-2}{0} = \infty$ *Identity element.*

d. $\frac{(p-1) \cdot (p-1) - 1}{(p-1)+(p-1)} = \frac{p^2 - 2 \cdot p + 1 - 1}{2 \cdot (p-1)} = \frac{0}{2 \cdot (p-1)}$ *Identity element.*

Algorithm 1 *group_operation*(x_1, x_2, N)

```
xs ← x1 + x2
gc ← gcd(xs, N) {gcd(0, N) = N}
if gc ≠ 1 then
   if gc=N then
      return (0)
   else
      return (-gc)
   end if
end if
return (((x1 · x2 − 1)/xs)(mod N))
```

Note 1. *If we want to avoid using* ∞ *in the* (6) *we can implement a group operation in the following way:*

$$x_1 * x_2 = \begin{cases} 0 & \textit{if} \quad x_1 + x_2 = 0 \\ \frac{x_1 x_2 - 1}{x_1 + x_2} & \textit{if} \quad x_1 + x_2 \neq 0 \end{cases} \tag{12}$$

By introducing this operation, the identity element would not be an unordered pair.

3 Primality test

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

$$2^{N-1} \equiv 1 \pmod{N} \tag{13}$$

and

$$2^{(N+1)/2} = \textit{identity element} \tag{14}$$

In equation (13), the group operation is $x_3 \equiv x_1 x_2 \pmod{N}$
In equation (14), the group operation is $x_3 \equiv \frac{x_1 x_2 - 1}{x_1 + x_2} \pmod{N}$

1	2	3	4	5
fer	$4k+1$	$4k-1$	$fer \cap 4k+1$	$fer \cap 4k-1$
341	8321	527	8321	$\emptyset$
561	24769	1679	721801	
645	25481	2627	2491637	
1105	38081	3599	2977217	
1387	40501	3827	4181921	
1729	64261	18527	6749021	
1905	84001	20099	7232321	
2047	164833	32239	7306261	
2465	172789	32399	9863461	
2701	195841	37127	10386241	
2821	214369	39059	20234341	
3277	257581	48827	35851037	
4033	270293	60959	37439201	
4369	280393	79799	37469701	
4371	289301	80999	43363601	
4681	349441	83711	44314129	
5461	404801	97663	46517857	
6601	416641	100127	47253781	
7957	496801	115639	47903701	
8321	518977	117739	48551161	
8481	544321	130591	51283501	
8911	561601	155819	60696661	

Table 1: In column one are a Fermat pseudoprime to the bases 2
In column two are a $4k+1$ pseudoprime to the bases 2
In column three are a $4k-1$ pseudoprime to the bases 2
In column four is intersection $fer \cap 4k+1$
In column five is intersection $fer \cap 4k-1$

In [11] compressed text files present data on all base-2 Fermat pseudoprimes below 2^{64}. The hypothesis to primality test was verified up to $N = 2^{64}$.

The computational complexity of the primality test can be divided into two parts:
1. The computational complexity of an exponentiation, which is the same for each group [5].
2. The computational complexity of a group operation $*$.
Computational complexity of mathematical operations [13, 14].

We do not compare the primality tests, there is rich literature - for example [1, 3, 4, 5, 15, 16].

One of the possible ideas of proof may be based on the fact that the $4k-1$ and $(Z/pZ)^*$ groups differ in structure, the number of elements is different.
Next, we looking for necessary condition that the number $N = 4k-1$ is a Fermat pseudoprime.
Next, we looking for necessary condition that the number $N = 4k-1$ is a $4k-1$ pseudoprime.
Finally, we show that these two necessary conditions can not be met at all together. Intersection of a Fermat pseudoprime and $4k-1$ pseudoprime is empty set.

4 Conclusion

Group operation (6) can be generalized as follows:

$$x_3 \equiv \frac{x_1x_2 + c}{x_1 + x_2} \pmod p \tag{15}$$

Next, there is the table (2) for the constant c [12]. From of the table is easy to see when the group will have $\frac{p-1}{2}$ or $\frac{p+1}{2}$ elements. A similar hypothesis can be proposed to testing many numbers.

We came on the group operation $\frac{x_1x_2-1}{x_1+x_2}$ when we worked with special binary quadratic forms [2] [9].

Another application of the new Abelian groups is in use for integer factorization and for public-key cryptosystems[9].

In appendix A are a powers of an element of a group of p = 17 and p = 19.

In appendix B is the code for the power in language pari/gp.

In the future, we will publish a more detailed article.

c	c is a quadratic residue mod p if and only if	c	c is a quadratic residue mod p if and only if
1	every prime p	-1	$p \equiv 1 (\bmod 4)$
2	$p \equiv 1, 7 (\bmod 8)$	-2	$p \equiv 1, 3 (\bmod 8)$
3	$p \equiv 1, 11 (\bmod 12)$	-3	$p \equiv 1 (\bmod 3)$
4	every prime p	-4	$p \equiv 1 (\bmod 4)$
5	$p \equiv 1, 4 (\bmod 5)$	-5	$p \equiv 1, 3, 7, 9 (\bmod 20)$
6	$p \equiv 1, 5, 19, 23 (\bmod 24)$	-6	$p \equiv 1, 5, 7, 11 (\bmod 24)$
7	$p \equiv 1, 3, 9, 19, 25, 27 (\bmod 28)$	-7	$p \equiv 1, 2, 4 (\bmod 7)$
8	$p \equiv 1, 7 (\bmod 8)$	-8	$p \equiv 1, 3 (\bmod 8)$
9	every prime p	-9	$p \equiv 1 (\bmod 4)$
10	$p \equiv 1, 3, 9, 13, 27, 31, 37, 39 (\bmod 40)$	-10	$p \equiv 1, 7, 9, 11, 13, 19, 23, 37 (\bmod 40)$
11	$p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 (\bmod 44)$	-11	$p \equiv 1, 3, 4, 5, 9 (\bmod 11)$
12	$p \equiv 1, 11 (\bmod 12)$	-12	$p \equiv 1 (\bmod 3)$

Table 2: Quadratic residue

A Integral Powers of an Element of a Group

The group operation is $x_3 \equiv \frac{x_1 x_2 - 1}{x_1 + x_2} \pmod{p}$

x and $\frac{-1}{x}$ are equals elements.

$p = 17 \quad a = 2 \quad$ order of a is 8		
$exponent$	$x = a^{exponent}$	$\frac{-1}{x}$
1	2	8
2	5	10
3	11	3
4	16	1
5	14	6
6	7	12
7	9	15
8	0	
9	8	2
10	10	5
11	3	11
12	1	16
13	6	14
14	12	7
15	15	9
16	0	
17	8	2
18	5	10
19	11	3
20	16	1
21	14	6
22	7	12
23	9	15
24	0	

Table 3: p=17,a=2

$p = 19 \quad a = 3 \quad$ order of a is 10		
$exponent$	$x = a^{exponent}$	$\frac{-1}{x}$
1	3	6
2	14	4
3	8	7
4	9	2
5	18	1
6	17	10
7	12	11
8	15	5
9	13	16
10	0	
11	6	3
12	4	14
13	7	8
14	2	9
15	1	18
16	10	17
17	11	12
18	5	15
19	16	13
20	0	
21	6	3
22	14	4
23	8	7
24	9	2
25	18	1
26	17	10
27	12	11
28	15	5
29	13	16
30	0	

$p = 19 \quad a = 2 \quad$ order of a is 5		
$exponent$	$x = a^{exponent}$	$\frac{-1}{x}$
1	2	9
2	15	5
3	14	4
4	10	17
5	0	
6	9	2
7	5	15
8	4	14
9	17	10
10	0	
11	9	2
12	15	5
13	14	4
14	10	17
15	0	
16	9	2
17	5	15
18	4	14
19	17	10
20	0	
21	9	2
22	15	5
23	14	4
24	10	17
25	0	

Table 4: p=19,a=2,a=3

B Code

This algorithm will compute the exponentiation and language pari/gp [10] is used.

```
power(N,y,ex)={
      local(i,bex,y0);

      bex=binary(ex);
      y0=y;
      for(i=2,matsize(bex)[2],
            if(bex[i],
                  y=group_operation(y,y,N);
                  if(y<0,return(y));
                  y=group_operation(y,y0,N);
                  if(y<0,return(y));
            ,
                  y=group_operation(y,y,N);
                  if(y<0,return(y));
            );
      );
      return(y);
}
```

References

[1] Daniel J. Bernstein, *Distinguishing Prime Numbers from Composite numbers: The State of the Art in 2004* Department of Mathematics, Statistics, and Computer Science (M/C 249), The University of Illinois at Chicago, Chicago, IL 60607 7045

[2] J. Buchmann and U. Vollmer, *Binary quadratic forms: An algorithmic approach*, Algorithms and Computation in Mathematics, vol. 20, Springer-Verlag, Berlin, 2007.

[3] Richard Crandall, Carl Pomerance, *Prime Numbers - A Computational Perspective* © 2005 Springer Science+Business Media, Inc.

[4] Paulo Ribenboim *The Little Book of Bigger Primes*, Second Edition, © 2004 Springer-Verlag New York, Inc.

[5] Song Y. Yan, *Number Theory for Computing* Springer-Verlag Berlin Heidelberg (2000)

[6] https://alexandrianlibers.files.wordpress.com/2009/10/20377572-tarski-introduction-to-logic-and-to-the-methodology-of-the-deducti pdf

[7] http://mathworld.wolfram.com/EquivalenceClass.html

[8] https://www.math.u-bordeaux.fr/~hecohen/rabinslides.dvi

[9] http://www.cryptoslovak.sk/

[10] https://pari.math.u-bordeaux.fr/

[11] http://www.cecm.sfu.ca/Pseudoprimes/index-2-to-64.html

[12] https://en.wikipedia.org/wiki/Quadratic_residue

[13] https://en.wikipedia.org/wiki/Computational_complexity_of_mathematical_operations

[14] https://en.wikipedia.org/wiki/Greatest_common_divisor

[15] https://en.wikipedia.org/wiki/Primality_test

[16] https://en.wikipedia.org/wiki/Baillie-PSW_primality_test

[17] https://en.wikipedia.org/wiki/Cyclic_group

[18] http://dogschool.tripod.com/cyclic.html

[19] https://en.wikipedia.org/wiki/Subgroups_of_cyclic_groups