An. Şt. Univ. Ovidius Constanţa Vol. 15(1), 2007, 97–104

A GENERALIZATION OF A RESULT OF FERMAT

Alexandru Gica

Abstract

The aim of this paper is to generalize a result of Fermat. For a prime p, we find all the nonnegative integers a such that $0 \leq a \leq 4p-1$ and $4pk+a$ does not divide p^n+1 for all nonnegative integers k, n.

A tribute: *I was not a student of Professor D. Popescu and I am not working in the same field as him, but we were colleagues for several years. I admire his exactingness, his critical sense, the fact that he is a hard working person and that he succeeded in the task of preserving the community centered around the "'Algebra Seminar"' (carrying on further the activity of Professor Nicolae Radu). It is also worthy to mention that he guided many younger mathematicians in their research.*

1 Introduction

Fermat proposed the following statement: there are no prime divisors $p = 12k + 11$ of the number $3^n + 1$. Fermat did not provide a proof for this statement. In 1929 S. S. Pillai proved a more general result: there are no positive divisors 12k+11 of the number $3^n + 1$.

The main aim of this paper is to solve the following problem.

Key Words: Fermat, quadratic reciprocity law
2000 Mathematical Subject Classification: 11A15, 11N13
Received: January, 2007

Problem. *Let p be a prime number. Which are the numbers a such that $0 \leq a \leq 4p-1$ and that $4pk+a$ does not divide p^n+1 for any nonnegative integers k, n?*

We dealt with some cases of this problem in [1] (Chapter 10, Problem no. 33) and in [2]. The tools for solving this problem are quadratic reciprocity law and the theorem of Dirichlet concerning the primes in an arithmetical progression.

2 The case p=2

This is the easiest case. We will show the following result.

Theorem 1. *Let $a \in \{0, 1, 2...7\}$. Then $8k+a$ does not divide 2^n+1 for all nonnegative integers k, n only for the values $a = 0, 4, 6, 7$.*

Proof. The only case which is worthy to prove is $a = 7$. Let us suppose that the statement is not true and that there exist $n, k \in \mathbb{N}$ such that $8k+7|2^n+1$. Let us consider the standard decomposition of $8k+7 = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. We have

$$2^n \equiv -1 \pmod{p_i}, \forall i = \overline{1,r}.$$

If n is even then -1 is quadratic residue modulo p_i $\forall i \in \overline{1,r}$. We obtain that $p_i \equiv 1 \pmod 4$ $\forall i = \overline{1,r}$ and that $8k+7 = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \equiv 1 \pmod 4$, which is obvious a contradiction.

If n is odd, then

$$-2 \equiv (2^{\frac{n+1}{2}})^2.$$

It results that $\left(\frac{-2}{p_i}\right) = 1$ and that $p_i \equiv 1, 3 \pmod 8 \forall i = \overline{1,r}$. We obtain the contradiction $8k+7 \equiv 1, 3 \pmod 8$.

3 The case $p \equiv 1 \pmod 4$

We will show the following result.

Theorem 2. *Let p be a prime number $p \equiv 1 \pmod 4$ and a a nonnegative integer such that $0 \leq a \leq 4p-1$. The numbers p^n+1 are not multiples of $4pk+a, \forall k, n$ nonnegative integers only for*

i) $p|a$ or

ii) $4|a$ or

iii) $a \equiv 3 \pmod 4$ and $\left(\frac{a}{p}\right) = 1$

Proof. If $i)$ or $ii)$ holds, then the statement of the theorem is obvious. Let us suppose now that the case $iii)$ holds and the statement of the theorem is not true; that is, there exist the nonnegative integers n, k such that $4pk + a | p^n + 1$. Let us consider the standard decomposition of $4pk + a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. We have

$$p^n \equiv -1 \pmod{p_i}, \forall i = \overline{1, r}.$$

If n is even then -1 is a quadratic residue modulo p_i $\forall i = \overline{1, r}$. We obtain that $p_i \equiv 1 \pmod 4$ $\forall i = \overline{1, r}$ and that $4pk + a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \equiv 1 \pmod 4$, which is an obvious contradiction since $4pk + a \equiv a \equiv 3 \pmod 4$. If n is odd, then

$$-p \equiv (p^{\frac{n+1}{2}})^2 \pmod{p_i}.$$

It results that $\left(\frac{-p}{p_i}\right) = 1$ and that $\left(\frac{p_i}{p}\right) = \left(\frac{p}{p_i}\right) = \left(\frac{-1}{p_i}\right)$ $\forall i = \overline{1, r}$. We obtain the following equalities

$$1 = \left(\frac{a}{p}\right) = \left(\frac{4pk + a}{p}\right) = \prod_{i=1}^{r} \left(\frac{p_i}{p}\right)^{\alpha_i} = \prod_{i=1}^{r} \left(\frac{-1}{p_i}\right)^{\alpha_i} = \left(\frac{-1}{4pk + a}\right) = -1.$$

We obtained a contradiction. In the previous formulas we used also the Jacobi symbol, the fact that $a \equiv 3 \pmod 4$ and $\left(\frac{a}{p}\right) = 1$. In the sequel we will show that the remaining cases are not solutions for our problem.

1. The case a odd, not multiple of p and quadratic nonresidue modulo p. Since $(4p, a) = 1$, we know from the theorem of Dirichlet that there is a prime q such that $q = 4pk + a$, where k is a nonnegative integer. From Euler's Criterion, we know that

$$p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{a}{p}\right) = -1 \pmod q.$$

Therefore we have that $q = 4pk + a$ divides $p^{\frac{q-1}{2}} + 1$ and a is not a solution for our problem.

2. The case $a \equiv 1 \pmod 4$, not multiple of p and quadratic residue modulo p. Let b be an integer which is not a multiple of p and quadratic nonresidue modulo p. Using the theorem of Dirichlet and the Chinese remainder theorem, we find two different primes p_1 and p_2 such that $p_1 \equiv b \pmod p, p_1 \equiv 3 \pmod 4, bp_2 \equiv a \pmod p, p_2 \equiv 3 \pmod 4$. We have $p_1 p_2 \equiv a \pmod{4p}$, $p_1 p_2 = 4pk + a$, where k is a nonnegative integer. We choose $n = \frac{p_1 - 1}{2} \cdot \frac{p_2 - 1}{2}$ which is an odd positive integer. Using again Euler's Criterion, we obtain

$$p^{\frac{p_1 - 1}{2}} \equiv \left(\frac{p}{p_1}\right) = \left(\frac{p_1}{p}\right) = \left(\frac{b}{p}\right) = -1 \pmod{p_1}$$

and

$$p^{\frac{p_2-1}{2}} \equiv \left(\frac{p}{p_2}\right) = \left(\frac{p_2}{p}\right) = \left(\frac{b}{p}\right)\left(\frac{bp_2}{p}\right) = -\left(\frac{a}{p}\right) = -1 \pmod{p_2}.$$

We have $p^n = (p^{\frac{p_1-1}{2}})^{\frac{p_2-1}{2}} \equiv (-1)^{\frac{p_2-1}{2}} = -1 \pmod{p_1}$. We used the above congruences and the fact that $p_2 \equiv 3 \pmod 4$. In the same way we prove that $p^n \equiv -1 \pmod{p_2}$. We have $4pk + a = p_1 \cdot p_2 | p^n + 1$ and this proves that this a is not a solution for our problem.

3. The case $a \equiv 2 \pmod 4$, not multiple of p, $a = 2b$ and b is quadratic nonresidue modulo p.

Since $(2p, b) = 1$, we know from the theorem of Dirichlet that there is a prime q such that $q = 2pk + b$, where k is a nonnegative integer. From Euler's Criterion, we know that

$$p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{b}{p}\right) = -1 \pmod q.$$

From here we have $2q = 4pk + a$ divides $p^{\frac{q-1}{2}} + 1$ and a is not a solution for our problem.

4. The case $a \equiv 2 \pmod 4$, not a multiple of p, $a = 2b$ and b is quadratic residue modulo p. Let c be an integer which is not a multiple of p and a quadratic nonresidue modulo p. Using the theorem of Dirichlet and the Chinese remainder theorem, we find two different primes x, y such that $x \equiv c \pmod p, x \equiv 3 \pmod 4, cy \equiv b \pmod p, y \equiv 3 \pmod 4$. We have $2xy \equiv a \pmod{4p}, 2xy = 4pk+a$, where k is a nonnegative integer. We choose $n = \frac{x-1}{2} \cdot \frac{y-1}{2}$ which is an odd positive integer. Reasoning like in the case 2. we obtain that $4pk + a = 2xy | p^n + 1$ and this proves that a is not a solution for our problem.

Remark: In the case $p \equiv 1 \pmod 4$, we have $4 + (p-1) + \frac{p-1}{2} = \frac{3p+5}{2}$ numbers a with the property stated in the theorem.

4 The case $p \equiv 3 \pmod 4$

Theorem 3. *Let p be a prime number $p \equiv 3 \pmod 4$ and a be a nonnegative integer such that $0 \le a \le 4p - 1$. The numbers $p^n + 1$ are not multiples of $4pk + a, \forall k, n$ nonnegative integers only for*

i) $p | a$ or

ii) $a = 4t$ and $\left(\frac{t}{p}\right) = -1$ or

iii) $a \equiv 3 \pmod 4$ and $\left(\frac{a}{p}\right) = -1$

Proof. If $i)$ holds, then the statement of the theorem is obvious. Let us suppose now that the case $ii)$ holds and the statement of the theorem is not true; that is, there exist $0 \leq a \leq 4p-1, a = 4t, \left(\frac{t}{p}\right) = -1$, n, k nonnegative integers such that $4pk + a | p^n + 1$. Let us consider the standard decomposition of $4pk + a = 2^t \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r}; t \geq 2$. We have $p^n \equiv -1 \pmod 4$ and therefore n is odd. We have

$$p^n \equiv -1 \pmod{p_i}, \forall i = \overline{1, r}.$$

Then

$$-p \equiv (p^{\frac{n+1}{2}})^2 \pmod{p_i}.$$

It results that $\left(\frac{-p}{p_i}\right) = 1$ and that $\left(\frac{p_i}{p}\right) = \left(\frac{-p}{p_i}\right) = 1 \ \forall i = \overline{1, r}$. We obtain the following equalities

$$-1 = \left(\frac{t}{p}\right) = \left(\frac{4t}{p}\right) = \left(\frac{a}{p}\right) = \left(\frac{4pk + a}{p}\right) = \left(\frac{2}{p}\right)^t \prod_{i=1}^{r} \left(\frac{p_i}{p}\right)^{\alpha_i} = \left(\frac{2}{p}\right)^t = 1.$$

The last equality holds obviously if $p \equiv 7 \pmod 8$. If $p \equiv 3 \pmod 8$, then $p^n + 1 \equiv 4 \pmod 8$ and therefore $t = 2$. This explains why the last equality holds in this case. We obtained a contradiction. Let us suppose now that the case $iii)$ holds and the statement of the theorem is not true; that is, there exist the integer a such that $a \equiv 3 \pmod 4$, $\left(\frac{a}{p}\right) = -1$ and the nonnegative integers n, k such that $4pk + a | p^n + 1$. Let us consider the standard decomposition of $4pk + a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. We have

$$p^n \equiv -1 \pmod{p_i}, \forall i = \overline{1, r}.$$

If n is even, then -1 is quadratic residue modulo p_i $\forall i = \overline{1, r}$. We obtain that $p_i \equiv 1 \pmod 4$ $\forall i = \overline{1, r}$ and that $4pk + a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \equiv 1 \pmod 4$, which is obvious a contradiction, since $4pk + a \equiv a \equiv 3 \pmod 4$. If n is odd, then

$$-p \equiv (p^{\frac{n+1}{2}})^2 \pmod{p_i}.$$

It results that $\left(\frac{-p}{p_i}\right) = 1$ and that $\left(\frac{p_i}{p}\right) = \left(\frac{-p}{p_i}\right) = 1 \ \forall i = \overline{1, r}$. We obtain the following equalities

$$-1 = \left(\frac{a}{p}\right) = \left(\frac{4pk + a}{p}\right) = \prod_{i=1}^{r} \left(\frac{p_i}{p}\right)^{\alpha_i} = 1.$$

We otained a contradiction. In the sequel we will show that the remaining cases are not solutions for our problem.

1. The case $a = 4t$, t is not a multiple of p and t is a quadratic residue modulo p. Since $(p, t) = 1$, we know from the theorem of Dirichlet and the Chinese remainder theorem that there is a prime $q \equiv 3 \pmod 4$ such that $q = pk + t$, where k is a nonnegative integer. From Euler's Criterion, we know that

$$p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) = -\left(\frac{t}{p}\right) = -1 \pmod q.$$

From here we have $4q = 4pk + a$ divides $p^{\frac{q-1}{2}} + 1$ and a is no solution for our problem.

2. The case $a \equiv 3 \pmod 4$, a is not a multiple of p and a quadratic residue modulo p. Since $(p, a) = 1$, we know from the theorem of Dirichlet and the Chinese remainder theorem that there is a prime q such that $q \equiv 3 \pmod 4$ and $q \equiv a \pmod p$. We have $q \equiv a \pmod{4p}$ and $q = 4pk + a$, where k is a nonnegative integer. From Euler's Criterion, we know that

$$p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) = -\left(\frac{a}{p}\right) = -1 \pmod q.$$

From here we have $q = 4pk + a$ divides $p^{\frac{q-1}{2}} + 1$ and a is no solution for our problem.

3. The case $a \equiv 1 \pmod 4$, not multiple of p and quadratic non-residue modulo p. Since $(p, a) = 1$, we know that there is a prime q such that $q \equiv 1 \pmod 4$ and $q \equiv a \pmod p$. We have $q \equiv a \pmod{4p}$ and $q = 4pk + a$, where k is a nonnegative integer. From Euler's Criterion we know that

$$p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{a}{p}\right) = -1 \pmod q.$$

From here we have $q = 4pk + a$ divides $p^{\frac{q-1}{2}} + 1$ and a is not a solution for our problem.

4. The case $a \equiv 1 \pmod 4$, is not a multiple of p and a quadratic residue modulo p. Let b be an integer which is not a multiple of p and quadratic nonresidue modulo p. We find two different primes p_1 and p_2 such that $p_1 \equiv 1 \pmod p, p_1 \equiv 3 \pmod 4, p_2 \equiv a \pmod p, p_2 \equiv 3 \pmod 4$. We have $p_1 p_2 \equiv a \pmod{4p}$, $p_1 p_2 = 4pk + a$, where k is a nonnegative integer. We choose $n = \frac{p_1 - 1}{2} \cdot \frac{p_2 - 1}{2}$ which is an odd positive integer. Using again Euler's Criterion, we obtain

$$p^{\frac{p_1-1}{2}} \equiv \left(\frac{p}{p_1}\right) = -\left(\frac{p_1}{p}\right) = -\left(\frac{1}{p}\right) = -1 \pmod{p_1}$$

and

$$p^{\frac{p_2-1}{2}} \equiv \left(\frac{p}{p_2}\right) = -\left(\frac{p_2}{p}\right) = -\left(\frac{a}{p}\right) = -1 \pmod{p_2}.$$

We have $p^n = (p^{\frac{p_1-1}{2}})^{\frac{p_2-1}{2}} \equiv (-1)^{\frac{p_2-1}{2}} = -1 \pmod{p_1}$. We used the above congruences and the fact that $p_2 \equiv 3 \pmod 4$. In the same way, we prove that $p^n \equiv -1 \pmod{p_2}$. We have $4pk + a = p_1 \cdot p_2 | p^n + 1$ and this proves that a is not a solution for our problem.

5. The case $a \equiv 2 \pmod 4$, is not a multiple of p, $a = 2b$ and b is a quadratic residue modulo p. Since $(p, b) = 1$, we know from the theorem of Dirichlet and the Chinese remainder theorem that there is a prime q such that $q \equiv 3 \pmod 4$ and $q \equiv b \pmod p$. We have $2q \equiv a \pmod{4p}$ and $2q = 4pk + a$, where k is a nonnegative integer. From Euler's Criterion we know that

$$p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) = -\left(\frac{b}{p}\right) = -1 \pmod q.$$

From here, we have $2q = 4pk + a$ divides $p^{\frac{q-1}{2}} + 1$ and a is not a solution for our problem.

6. The case $a \equiv 2 \pmod 4$, not multiple of p, $a = 2b$ and b is quadratic nonresidue modulo p. Since $(p, b) = 1$, we know that there is a prime q such that $q \equiv 1 \pmod 4$ and $q \equiv b \pmod p$. We have $2q \equiv a \pmod{4p}$ and $2q = 4pk + a$, where k is a nonnegative integer. From Euler's Criterion we know that

$$p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{b}{p}\right) = -1 \pmod q.$$

From here we have $2q = 4pk + a$ divides $p^{\frac{q-1}{2}} + 1$ and a is no solution for our problem.

Remark 1. In the case $p \equiv 3 \pmod 4$, we have $4 + \frac{p-1}{2} + \frac{p-1}{2} = p + 3$ numbers a with the property stated in the theorem.

Remark 2. If we put in Theorem 3 $p = 3$ and $a = 11$, we obtain the generalization of Fermat's result proved by S. S. Pillai

Acknowledgment: This work was supported in part by the CNCSIS grant 1068/2006.

References

[1] A. Gica, L. Panaitopol, *Aritmetică şi Teoria Numerelor.Probleme,* Editura Universităţii Bucureşti, 2006.

[2] A. Gica, *Asupra unei teoreme a lui Fermat,* Gazeta Matematică seria A, (1996), no. 4, 220–223.

Faculty of Mathematics and Computer Science,
University of Bucharest, Academiei 14,
010014 Bucharest, Romania
E-mail: gica@al.math.unibuc.ro