A Nice Lemma In Congruence

Masum Billal

November 3, 2015

Abstract

Thue's Lemma is a wonderful theorem in congruence. It should have been quite popular, but unfortunately it not only isn't very popular, it doesn't have many resources from olympiad perspective when searched in the internet, hence the article. In this article, we prove this lemma and show some nice applications related to sum of squares or quadratic residue. Thanks to anyone who helped in improving the article, specially to user **randomusername** for providing links, references of the problems and constructive suggestion. I have tried to keep the article as self contained as possible. If there are still something the reader does not know, it may be assumed that the topic is too common in AoPS.

1 Main Result

Theorem 1 (Thue's Lemma)**.** *Let $n > 1$ be an integer and a be an integer co-prime to n. Then there are integers x, y with $0 < |x|, |y| < \sqrt{n}$ so that*

$$x \equiv ay \pmod{n}$$

Such a solution (x, y) is called a small solution sometimes.

Proof. Let $r = \lfloor \sqrt{n} \rfloor$ i.e. r is the unique integer for which $r^2 \leq n < (r+1)^2$. The number of pairs (x, y) so that $0 \leq x, y \leq r$ is $(r+1)^2$ which is greater than n. Then there must be two different pairs (x_1, y_1) and (x_2, y_2) so that

$$\begin{aligned} x_1 - ay_1 &\equiv x_2 - ay_2 \pmod{n} \\ x_1 - x_2 &\equiv a(y_1 - y_2) \pmod{n} \end{aligned}$$

Let $x = x_1 - x_2$ and $y = y_1 - y_2$, and we get $x \equiv ay \pmod{n}$. Now, we need to show that $0 < |x|, |y| < r$ and $x, y \neq 0$. Certainly, if one of x, y is zero, the other is zero as well. If both x and y are zero, that would mean that two pairs (x_1, y_1) and (x_2, y_2) are actually same. That is not the case, and so both x, y can not be 0. Therefore, none of x or y is 0, and we are done. □

Corollary 1. *For a prime p and an integer a, there are integers x, y with $0 < |x|, |y| < \sqrt{p}$ such that*

$$x \equiv ay \pmod{p}$$

This lemma can be generalized even more with the same proof.

Theorem 2 (Generalization of Thue's Lemma)**.** *Let α and β are two real numbers so that $\alpha\beta \geq p$. Then for an integer x, there are integers a, b with $0 < |a| < \alpha$ and $0 < |b| < \beta$ so that,*

$$a \equiv xb \pmod{p}$$

And we can even make this lemma a two dimensional one.

Theorem 3 (Two Dimensional Thue's Lemma)**.** *Let $n \geq 2, r = \sqrt{n}$ and a, b, c, d be arbitrary integers. There exist w, x, y, z with at least one of y, z non-zero such that*

$$\begin{aligned} 0 \leq |w|, |x|, |y|, |z| &\leq r \\ w &\equiv ay + bz \pmod{n} \\ x &\equiv cy + dz \pmod{n} \end{aligned}$$

2 Applications

First we show an elegant proof of Fermat's $4n+1$ theorem here using a well known theorem and Thue's theorem (1).

Definition 1 (Bisquare)**.** The sum of two perfect squares which are co-prime to each other is a bisquare.

Definition 2 (Quadratic Residue)**.** a is a *quadratic residue* of a prime p if there exist an integer x so that,

$$x^2 \equiv a \pmod{p}$$

a is a quadratic non-residue if there doesn't exist any such integer x that,

$$x^2 \equiv a \pmod{p}$$

Definition 3. Two integers a and b are co-prime if their greatest common divisor $(a, b) = 1$. We denote this by $a \perp b$.

To prove Fermat's theorem, we will use the following theorem without proof, which is pretty well known and posted so many times on AoPS.

Theorem 4. *-1 is a quadratic residue of a prime p if and only if p is of the form $4n+1$.*

Theorem 5 (Fermat's $4n+1$ Theorem)**.** *Every prime of the form $4n+1$ can be written as a bisquare.*

Proof. We already know that, for $p \equiv 1 \pmod 4$, there is an x so that,

$$x^2 \equiv -1 \pmod{p}$$

From Thue's theorem, for such an x, there are integers a, b with $0 < |a|, |b| < \sqrt{p}$ so that,

$$\begin{aligned} a &\equiv xb \pmod{p} \\ a^2 &\equiv x^2b^2 \pmod{p} \\ &\equiv -b^2 \pmod{p} \\ a^2 + b^2 &\equiv 0 \pmod{p} \end{aligned}$$

The last congruence means that $p|a^2+b^2$, so

$$\begin{aligned} p &\leq a^2+b^2 \text{ but} \\ a^2+b^2 &< p+p \\ &= 2p \end{aligned}$$

Therefore, $a^2+b^2=p$ must occur.

□

In fact, we can use the same technique for generalizing *Fermat's* $4n+1$ *theorem.*

Theorem 6. *Let* $n \in \{-1,-2,-3\}$. *If* n *is a quadratic residue of a prime* p, *then there are integers* a, b *so that,* $a^2-nb^2=p$.

Proof. We have already proven the case $n=-1$. If n is a quadratic residue of p,

$$x^2 \equiv n \pmod{p}$$

has a solution. Fix the integer x, and take a, b as in Thue's lemma so that,

$$\begin{aligned} a &\equiv xb \pmod{p} \\ a^2 &\equiv x^2b^2 \pmod{p} \\ &\equiv nb^2 \pmod{p} \\ p|a^2-nb^2 & \end{aligned}$$

We make two cases for n.

- $n=-2$. Then $p \leq a^2+2b^2 < p+2p = 3p$. So, either $a^2+2b^2=p$ or $a^2+2b^2=2p$. If it's the first, we are done. If not, we see that a must be even. Assume $a=2a'$ and we get $p=b^2+2a'^2$, as desired.

- Now, $n=-3$, so $p \leq a^2+3b^2 < p+3p = 4p$. If $a^2+3b^2=2p$, then a and b are both odd or both even. If both are even, then $2p$ is divisible by 4, a contradiction since p is odd. Otherwise, a and b are both odd.

  $$\begin{aligned} a^2+3b^2 &\equiv 1+3\cdot 1 \pmod{4} \\ 2p &\equiv 0 \pmod{4} \end{aligned}$$

  Again, contradiction. We are left with the case $a^2+3b^2=3p$. This shows a is divisible by 3. If we take $a=3a'$, we get $p=b^2+3a'^2$.

□

Corollary 2. *For a prime p and an integer n, there exists integers x, y so that p divides $x^2 + ny^2$ with $p \not| x, y$ if and only if $-n$ is a quadratic residue of p.*

Proof. Without loss of generality, we can take x and y to be co-prime and n not divisible by p. First assume, $p|x^2 + ny^2$, then y must be co-prime to p. Therefore, y has an inverse modulo p, assume $ay \equiv 1 \pmod{p}$.

$$\begin{aligned} a^2y^2 &\equiv 1 \pmod{p} \\ p|a^2x^2 + na^2y^2 \\ p|a^2x^2 + n \\ (ax)^2 &\equiv -n \pmod{p} \end{aligned}$$

For the only if portion, we have $-n$ is a quadratic residue of p, let $k^2 \equiv -n \pmod{p}$. Clearly, $\gcd(k, p) = 1$ otherwise p will divide n. From Thue's lemma, there are integers x, y with

$$\begin{aligned} x &\equiv ky \pmod{p} \\ x^2 &\equiv k^2y^2 \pmod{p} \\ &\equiv -ny^2 \pmod{p} \\ p|x^2 + ny^2 \end{aligned}$$

□

We can use these results to imply the following theorem also.

Theorem 7. *For $D \in \{1, 2, 3\}$, if $n = x^2 + Dy^2$ for some $x \perp y$, then every divisor d of n is of the same form.*

Proof. Remember the identity:

$$\begin{aligned} (a^2 + Db^2)(c^2 + Dd^2) &= (ac - Dbd)^2 + D(ad + bc)^2 \\ &= (ac + Dbd)^2 + D(ad - bc)^2 \end{aligned}$$

This means that the product of two numbers of the form $x^2 + Dy^2$ is of the same form. From theorems above, if p is a divisor of $x^2 + Dy^2$, then $p = a^2 + Db^2$ for some a, b. The identity clearly says that, if $m = a^2 + Db^2$,

then any power of m, m^k is of this form again. Let's assume that, the prime factorization of n is,

$$\begin{aligned} n &= p_1^{e_1} \cdots p_k^{e_k} \\ &= \prod_{i=1}^{k} p_i^{e_i} \text{ and} \\ d &= \prod_{i=1}^{k} p_i^{f_i} \text{ where } 0 \leq f_i \leq e_i \end{aligned}$$

From the lemma, for any $1 \leq i \leq k$, p_i is of this form. So, $p_i^{f_i}$ is of the same form as well. So, for any divisor $p_1^{f_1} \cdot p_2^{f_2}$ is of the same form again. Repeating this upto $p_k^{f_k}$ we get that, $p_1^{f_1} \cdots p_k^{f_k} = d$ is of the same form again.

□

Now we prove another theorem that demonstrates the power of Thue's theorem. We will use the following theorem without proof.

Theorem 8. *-3 is a quadratic residue of p if and only if p is of the form $3k+1$.*

Theorem 9. *If p is a prime of the form $3k+1$, there are integers a, b such that $p = a^2 + ab + b^2$.*

Proof. Since p is of the form $3k+1$, -3 is a quadratic residue of p. Take y to be an odd integer for which $p|y^2+3$ or,

$$y^2 \equiv -3 \pmod{p}$$

Such an y exists, since p is odd. Even if y is even, $y \equiv 2x+1 \pmod{p}$ has a solution. For that x, we get,

$$\begin{aligned} (2x+1)^2 &\equiv -3 \pmod{p} \\ 4x^2 + 4x + 1 &\equiv -3 \pmod{p} \\ 4(x^2 + x + 1) &\equiv 0 \pmod{p} \\ x^2 + x + 1 &\equiv 0 \pmod{p} \end{aligned}$$

because p is odd. From Thue's theorem, there are integers a, b with $0 < |a|, |b| < p$ such that,

$$a \equiv xb \pmod{p}$$

Then we also get

$$\begin{aligned} a^2 + ab + b^2 &= a^2 + a \cdot ax + (ax)^2 \\ &= a^2(x^2 + x + 1) \\ &\equiv 0 \pmod{p} \end{aligned}$$

Because $p|a^2 + ab + b^2$, $p \leq a^2 + ab + b^2$. On the other hand,

$$\begin{aligned} p &\leq a^2 + ab + b^2 \\ &< p + p + p \\ &= 3p \end{aligned}$$

Either $a^2 + ab + b^2 = p$ or $a^2 + ab + b^2 = 2p$. We can easily check that $a^2 + ab + b^2 = 2p$ can not happen (try yourself).

□

3 Problems

Assume that you know Thue's lemma. How do we get that we need this particular lemma here? And how do we approach? If you saw the previous proof of the sum of squares theorems, you should understand the main advantage of using Thue's lemma. The idea of small solutions is crucial here. For that, we can bound some integers here.

Theorem 10. *Let $p > 5$ be a prime so that, p divides $k^2 + 5$ for some integer k. Show that, there are integers x, y such that, $p^2 = x^2 + 5y^2$.*

Problem 1. Let p be a prime for which there exists a positive integer a such that p divides $2a^2 - 1$. Prove that, there exist integers b and c so that, $p = 2b^2 - c^2$.

Solution. We have $2a^2 - 1 \equiv 0 \pmod{p}$. Since we want to bound $2b^2 - c^2$, it is obvious, we should find b, c so that p divides $2b^2 - c^2$ and then bound it. This is where Thue's lemma comes in. Fix the integer a, which is clearly co-prime to p. Then from Thue's lemma, we there are integers b, c with $0 < |b|, |c| < \sqrt{p}$ so that,

$$b \equiv ac \pmod{p}$$

This gives us what we need. Note that,

$$\begin{aligned} 2b^2 - c^2 &\equiv 2(ac)^2 - c^2 \\ &\equiv c^2(2a^2 - 1) \\ &\equiv 0 \pmod{p} \end{aligned}$$

Thus, p divides $2b^2 - c^2$, and now we get to use the fact:

$$\begin{aligned} p &\leq 2b^2 - c^2 \\ &< 2b^2 < 2p \end{aligned}$$

We immediately get that $p = 2b^2 - c^2$.

Problem 2 (Kömal)**.** Let n be an integer. Prove that if the equation $x^2 + xy + y^2 = n$ has a rational solution, then it also has an integer solution.

Problem 3 (Iran Olympiad, 3rd Round)**.** Let p be a prime number. Prove that, there exists integers x, y such that $p = 2x^2 + 3y^2$ if and only if $p \equiv 5, 11 \pmod{24}$.

Problem 4 (Polish Math Olympiad Problem)**.** Let S be a set of all positive integers which can be represented as $a^2 + 5b^2$ for some integers a, b such that $a \perp b$. Let p be a prime number such that $p = 4n+3$ for some integer n. Show that if for some positive integer k the number kp is in S, then $2p$ is in S as well.

Problem 5 (Kömal)**.** Prove that the equation $x^3 - x + 9 = 5y^2$ has no solution in integers.

References

[1] Kömal, Problem A 595, `http://www.komal.hu/verseny/feladat.cgi?a=feladat&f=A595&l=en`

[2] Kömal, Problem A 618, `http://www.komal.hu/verseny/feladat.cgi?a=feladat&f=A618&l=en`

[3] Kömal, Problem A 283, `http://www.komal.hu/verseny/2002-01/A.e.shtml`